CERTAIN GENERALIZATIONS OF PERMUTATION—INVARIANT SYSTEMS

A Thesis Submitted
In Partial Fulfilment of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY

By
PRAKRIYA RAMAKRISHNA RAO

to the
DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR
May, 1978

CERTIFICATE

Certified that this work 'CERTAIN GENERALIZATIONS OF PERMUTATION-INVARIANT SYSTEMS' by P. Rama Krishna Rao has been carried out under my supervision and that this has not been submitted elsewhere for a degree.

(V. P. SINHA)
Department of Electrical Engineering
Indian Institute of Technology
Kanpur

4.11.1978

ACKNOWLEDGEMENTS

I am grateful to my thesis supervisor, Dr. V.P. Sinha, for the overall guidance provided by him throughout the research work. Frequent discussions with him on various topics have gone a long way in shaping this thesis in the present form.

I also wish to place on record my thanks to all my friends who helped me in various ways in the preparation of this thesis.

Finally, I wish to thank Mrs. Rukmini Devi for the excellent typing work and also for the help rendered by her, in the processing of the thesis from the manuscript stage to the present form.

P. RAMA KRISHNA RAO

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SYNOPSIS

This thesis presents a generalized theory of permutation-invariant (P-I) systems that find applications in the processing of finite discrete data. The existing theory of such systems deals exclusively with only the one-dimensional kind which accept finite-length sequences of reals as their input signals and which are the finite discrete counterparts of one-dimensional (1-D) linear shift-invariant (LSI) systems. The material presented in this thesis is an extension and generalization of the existing theory and covers two-dimensional (2-D) P-I systems whose input signals are finite 2-D arrays of reals, and also those P-I systems whose input signals are finite-length sequences with entries drawn from finite fields and rings of residue class integers. Having features similar to those of 2-D LSI systems and linear sequential circuits, these new categories of P-I systems are expected to have analogous applications in signal processing.

A 1-D linear system whose input and output signals are finite sequences of some arbitrary length N, has ~~earlier~~ previously been defined to be permutation-invariant relative to a transitive abelian group of permutations G of order N, if the effect of permuting its input signal by any member of G is to permute the output signal also in the same manner. By analogy, a 2-D P-I system is defined here as a 2-D finite discrete linear system that exhibits invariance to certain kinds of permutations of the rows and columns of its input signal. To be

specific, let G_1 and G_2 be transitive abelian groups of permutations of orders m and n respectively. Then, a 2-D linear system which accepts input signals given by finite arrays or matrices having m rows and n columns, is defined to be permutation-invariant relative to the groups G_1 and G_2, if the effect of permuting the rows of its input signal by any member of G_1 and the columns of its input signal by any member of G_2 is to permute the output signal also exactly in the same manner. All 2-D P-I systems defined relative to the same pair of groups, G_1 for the rows and G_2 for the columns, are said to form a class of 2-D P-I systems relative to G_1 and G_2. A familiar example of 2-D P-I systems is provided by the 2-D cyclic convolutional systems which can be shown to have permutation-invariance property with respect to cyclic permutations.

The basic structural properties of 2-D P-I systems are expectedly the same as those of 1-D P-I systems except that they are centrally dependent upon two transitive abelian permutation groups rather than just one. Specifically, like the 1-D P-I systems, a class of 2-D P-I systems is characterized by a well-defined convolutional formula, a family of eigen vectors and a 2-D discrete transform. Each of these characterizations has been dealt with here in detail and several important results pertaining to them have been established. The arguments used in establishing these results are in spirit similar to those used in the case of 1-D P-I

systems. However, since the input and output signals of 2-D P-I systems are matrices rather than column vectors, a more formal approach has been used. In the present approach, signals are treated as members of the vector space V of real m x n matrices and systems are treated as linear transformations on this vector space. With signals and systems so treated, it is shown that a class of 2-D P-I systems defined relative to groups G_1 and G_2 forms a vector space whose dimension is the same as that of the pertinent signal space V of that class. Moreover, if B_{ij} denotes the transformation or operator whose action on any 2-D signal $X \varepsilon V$ is to permute its rows by the permutation $P_i \varepsilon G_1$ and the columns by the permutation $q_j \varepsilon G_2$, then the set of operators B_{ij}, $i \varepsilon Z_m$, $j \varepsilon Z_n$, where Z_k denotes the set of integers 0 to (k-1), forms a basis for this vector space. By recognizing that these B_{ij}'s are normal operators, it is shown that all 2-D P-I systems of a particular class have in common a set of N linearly independent orthonormal eigenvectors, where N = m.n. This equivalently means that each class of 2-D P-I systems has associated with it, a 2-D finite discrete transform (2-D FDT) which leads to the notion of transfer functions for 2-D P-I systems. In essence a generalization of the 2-D discrete Fourier and Walsh transforms (2-D DFT and 2-D DWT), the 2-D FDT for every class satisfies a generalized convolution theorem.

After developing the theory of 2-D P-I systems as an independent entity, attention is given to the relationships between 2-D and 1-D P-I systems. A key result in this context is that, for every class of 2-D P-I systems, there is an equivalent class of 1-D P-I systems. This result is obtained in three stages. Firstly, methods are examined for transforming 2-D signals into 1-D signals with the help of appropriate one-to-one index mappings $f: Z_m \times Z_n \rightarrow Z_N$, $N = m.n$. Next, considering an arbitrary 2-D signal $X \varepsilon V$, it is shown that permuting its rows and columns respectively by members of transitive abelian groups of permutations G_1 and G_2 is in effect the same as permuting the equivalent 1-D signal $x \varepsilon R^N$ by the members of the transitive abelian permutation group G which is characterized to within an isomorphism by the external direct product of G_1 and G_2. A general procedure for constructing the members of G, valid for any one-to-one index mapping $f: Z_m \times Z_n \rightarrow Z_N$, has been outlined by writing down kronecker products of matrices in such a way that the rows and columns of the product matrix are ordered not lexicographically, but in accordance with the pertinent index mapping f under consideration. Utilizing these results, it is finally shown that every member of a class of 2-D P-I systems defined relative to G_1 and G_2 has an equivalent 1-D P-I system defined relative to G.

The fact that every 2-D P-I system has an equivalent 1-D P-I system gives rise to interesting possibilities in the processing of 2-D finite discrete data. It is to be noted that the design of stable 2-D LSI systems and 2-D digital filters directly from 2-D specifications is beset with problems of spectral factorization of polynomials in two variables. A number of methods have therefore been proposed in the past for the design and implementation of 2-D digital filters indirectly by using 1-D techniques. These methods, however, are limited in their effectiveness by the fact that the exact 1-D implementation of a 2-D LSI system or a 2-D digital filter is a 1-D filter that does not possess the time-invariance property. As shown in this thesis, no such limitation exists in the case of P-I systems, in that, a 1-D system that is an exact equivalent of a given 2-D P-I filter retains the permutation-invariance property. Further, if the 2-D data to be processed are finite, a digital filter may be interpreted as a P-I filter, so that for finite discrete data, it is possible to convert a 2-D filtering problem into an exactly equivalent 1-D filtering problem by resorting to P-I system theory. These facts have been discussed in detail in the general context of filtering 2-D finite discrete data in Fourier and Walsh domains using P-I systems. 2-D Walsh domain filtering corresponds to 2-D dyadic P-I filtering, and the 1-D equivalent of a 2-D

dyadic P-I filter is a 1-D dyadic P-I filter. Likewise, it is shown that the 1-D equivalent of a 2-D Fourier domain filter is a 1-D cyclic P-I filter provided the number of rows and the number of columns of the pertinent 2-D signals are relatively prime.

Attention is next given to those P-I systems whose input sequences are of finite length n, with entries drawn from (i) finite fields, and (ii) rings of residue class integers. For convenience, these systems are respectively referred to as P-I systems on finite fields and P-I systems on rings. The main concern here is the transform domain theory of these systems, their sample domain behaviour being largely the same as that of 1-D P-I systems with real field inputs. The n-th roots of unity in finite fields and rings play an important role in the study of cyclic P-I systems of these types. The existence of these roots is accordingly first examined in detail and procedures for determining them are discussed. Cyclic P-I systems on finite fields and rings are then characterized in terms of their eigen signals and discrete transforms. These results for the cyclic class are then extended to general classes of these P-I systems and a characterization is given for them in terms of their respective eigen signals and generalized discrete transforms. It is observed that for appropriate choices of the modulus of the residue class ring,

the transforms defined by the corresponding class of cyclic P-I systems give rise to the so-called number-theoretic transforms (NTT's) such as the Mersenne number transform and the Fermat number transform. These NTT's have been proposed in the last few years primarily as a means of efficient and error-free computation of cyclic convolution. Looking at these transforms from ~~the~~ a system-theoretic point of view, it is shown in this thesis that just like the DFT and the DWT, the NTT's also have associated with them a specific class of P-I systems, the pertinent class of systems in this case being the class of cyclic P-I systems on rings of residue class integers. It is hoped that the generalized transforms derived here for different classes of P-I systems on rings would prove helpful in the evolution of newer varieties of NTT's having dyadic and such other non-cyclic convolutional properties.

CHAPTER 1

INTRODUCTION

1.1 Scope of the Work

In this thesis, certain generalizations of permutation-invariant linear systems (P-I systems) are studied. The existing theory of P-I systems deals exclusively with the one-dimensional (1-D) variety having real-field inputs. In other words, it deals only with those finite discrete linear systems which have finite sequences of reals as their input signals and which exhibit invariance to permutations of the input signal by members of a transitive abelian permutation group.

The generalizations studied in this thesis pertain to the following three new categories of P-I systems:

i. Two-dimensional (2-D) P-I systems which have finite 2-D arrays of reals as their input signals.

ii. P-I systems on finite fields, i.e., those 1-D P-I systems whose finite-length input sequences have their entries drawn from finite fields, and

iii. P-I systems on rings, i.e., those 1-D P-I systems whose finite-length input sequences have their entries from rings of residue class integers.

The motivation for the extensions covered by the first two categories, viz., 2-D P-I systems and P-I systems on finite fields, is provided by the fact that in the case of the linear shift-invariant (LSI) discrete-time systems, which originally served as the model for developing 1-D P-I systems [1] , there are in addition to the 1-D variety, two other equally important varieties whose theories are highly developed and well established. These are the 2-D LSI systems exemplified by 2-D digital filters and the finite field LSI systems exemplified by linear sequential circuits. Inasmuch as 1-D P-I systems are finite discrete counterparts of 1-D LSI systems, it is natural to expect the existence of 2-D P-I systems and finite field 1-D P-I systems with features similar respectively to those of 2-D LSI systems and finite field LSI systems and having roles analogous respectively to those of 2-D digital filters and linear sequential circuits.

The third category of P-I systems, viz., P-I systems on rings, is suggested by the so-called number-theoretic transforms (NTT's) that have been proposed during the last few years. These NTT's with discrete Fourier transform (DFT)-like

structure, have been proposed as computational aids for the purpose of efficient and error-free computation of cyclic convolutions. However, the fact that the DFT is associated with the cyclic class of 1-D P-I systems with real-field inputs, suggests that the NTT's also have associated with them, a specific category of P-I systems whose finite-length input sequences have entries from rings of residue class integers. Further, since the DFT turns out to be a special case of a larger family of generalized transforms defined by general classes of 1-D P-I systems with real field inputs, it is reasonable to conclude that a study of general classes of 1-D P-I systems of this new category would give rise to a more general family of number-theoretic transforms, which will include as a special case the present NTT's having cyclic convolutional property.

Historically, P-I systems have evolved as a generalization of the well-known cyclic and dyadic convolution systems [2, 3] and a comprehensive theory of various classes of 1-D P-I systems is available in [1]. A brief summary of this theory of P-I systems is given in Appendix A.

Of the various classes of 1-D P-I systems, only the cyclic and dyadic classes have been found to have a significant role in the processing of finite discrete data. The question then naturally arises whether the other classes of

1-D P-I systems have any useful role to play. As the results of this thesis show, most of those 1-D P-I systems which belong neither to the cyclic nor to the dyadic class are, in fact, the 1-D equivalents of two-dimensional or multidimensional cyclic or dyadic P-I systems. Thus, while these other classes of 1-D P-I systems may not directly be of use in the processing of 1-D signals, they are indirectly of practical use in the processing of two-dimensional and multidimensional finite discrete data. Several methods [6, 7, 8] have been suggested in the recent past for the use of 1-D techniques to achieve 2-D tasks in an attempt to overcome the problems of spectral factorization [8-12] arising in the design of stable 2-D digital filters directly from 2-D specifications. However, a basic limitation of all these methods is that the exact 1-D equivalent of a 2-D LSI system or a 2-D digital filter is a 1-D system that does not have the shift-invariance property [13]. A 1-D LSI realization of a 2-D digital filter can therefore be at best an approximation. As the results of this thesis show, no such basic limitation exists in the case of P-I systems and when the data to be processed ~~are~~ is finite, exact 1-D realizations of 2-D filters can be obtained using the P-I system approach.

Computation of convolutions via the DFT became attractive following the availability of the fast Fourier transform (FFT) algorithm [14]. However, the DFT involves complex

multiplications and additions that are inherently slow and inaccurate. The fast Fourier transform in finite fields [15] and the various NTT's [16-18] have been proposed in the last few years mainly as computational aids that avoid the deficiencies of the DFT mentioned earlier. Research work on these transforms appears to be wholly directed towards their computational aspects [19-21] rather than a system-based study of these transforms. By using a system-theoretic approach, it is shown in this thesis that all these transforms are special cases of certain generalized transforms defined by P-I systems on finite fields and on rings.

1.2 Outline of Chapters

The notion of permutation-invariance in two dimensions is introduced in Chapter 2 making use of the relevant concepts pertaining to the 1-D P-I systems as guide lines. The input and output signals for 2-D P-I systems are finite 2-D arrays or matrices while those for 1-D P-I systems are n-tuples or column vectors. Therefore, two transitive abelian permutation groups G_1 and G_2 of appropriate orders, with G_1 for the set of rows and G_2 for the set of columns, are used for defining a class of 2-D P-I systems. Specifically, such a class defined relative to the pair of groups G_1 and G_2 comprises the set of all 2-D finite discrete linear systems which exhibit invariance in their input-output behaviour, to

permutations of the rows and columns of their input signals by members of G_1 and G_2 respectively. Characterization of each class of these 2-D P-I systems is then obtained in terms of a convolutional formula, and a common set of linearly independent orthonormal eigenvectors which span the pertinent signal space for that class. In obtaining these results, owing to the fact that the input and output signals for 2-D P-I systems are matrices rather than column vectors, a more formal approach than what was needed in the 1-D case, has been used. In this approach, signals are treated as members of a vector space and systems are treated as operators on this vector space.

Relationships between 2-D and 1-D P-I systems are examined in Chapter 3. A significant result obtained in this context is that for every class of 2-D P-I systems, there is a corresponding class of 1-D P-I systems. As a first step in obtaining this result, some convenient methods are suggested for obtaining an equivalent 1-D signal $x \varepsilon R^N$ for a given 2-D signal $X \varepsilon V$, the space of real m x n matrices, in terms of appropriate one-to-one index mappings $f: Z_m \times Z_n \to Z_N$; $N = m.n$, which could also be interpreted as linear transformations $Q: V \to R^N$. Next, it is shown that the effect of permuting the rows and columns of a 2-D signal $X \varepsilon V$ by some arbitrary members of G_1 and G_2 respectively, is the same as permuting the equivalent 1-D signal $x \varepsilon R^N$ by the corresponding

member of a set of N permutation matrices. This set of permutation matrices is then shown to form a transitive abelian permutation group G which is isomorphic to the direct product of G_1 and G_2. Utilizing these results, it is finally shown that for every member of a class of 2-D P-I systems defined relative to G_1 and G_2, there is an equivalent 1-D P-I system in a class defined relative to G. A method for constructing the members of G is outlined. In this method, which makes it possible to provide a unified treatment of the results pertaining to 2-D to 1-D equivalence, Kronecker products of matrices are written down following an ordering of indices that corresponds to the pertinent index mapping f under consideration. Finally we obtain expressions for the eigenvalues and eigenvectors of an equivalent 1-D P-I system in terms of those of a given 2-D P-I system.

Chapter 4 deals with the transform domain description of 2-D P-I systems. Expectedly, the various results obtained here follow essentially the same pattern as the corresponding results for 1-D P-I systems. The result obtained in Chapter 2, that a class of 2-D P-I systems has a common set of linearly independent orthonormal eigenvectors that span the pertinent signal space for that class, is utilized here to derive generalized 2-D finite discrete transforms (2-D FDT). It is shown that the familiar 2-D DFT and 2-D DWT are special cases

of the 2-D FDT. Also, just as ~~the~~ 2-D DFT and 2-D DWT satisfy convolutional theorems pertaining to their respective classes, ~~the~~ 2-D FDT also satisfies a generalized convolutional theorem. The 2-D FDT associated with each class leads to the notion of transfer functions for 2-D P-I systems.

In Chapter 5, the idea of using 2-D P-I systems for filtering 2-D finite discrete data is explained. Besides discussing various aspects of 2-D P-I filtering in general, particular attention is given to the separable type of 2-D P-I filters. Their sample domain and transform domain behaviour, and their characterizations are also discussed. Methods for designing separable 2-D P-I filters are examined and examples illustrating the implementation of separable filters of cyclic and dyadic classes are given.

Chapter 6 deals with a general method of 1-D implementation of 2-D P-I filters with special reference to the cyclic and dyadic classes. This method of 1-D implementation is applicable irrespective of whether the given 2-D P-I system is separable or not and it is based on the results obtained in Chapter 3 concerning the equivalence between 2-D and 1-D P-I systems. Appropriate index mappings required for obtaining the equivalent 1-D P-I system have been derived

for each of these classes of systems and a number of examples are given illustrating the various techniques involved in this method of implementation.

Two new categories of 1-D P-I systems are considered in Chapter 7. These are 1-D P-I systems whose input sequences of some finite length n have their entries from (i) finite fields and (ii) rings of residue class integers. The main emphasis here is on the transform domain properties of these systems since it is in this domain that they differ from the 1-D P-I systems with real field inputs. First, cyclic classes of systems of these categories are considered and their characterizations in terms of finite discrete transforms, are obtained. As the eigenvectors of the cyclic class of systems have the n-th roots of unity as their entries, the question of existence of these roots in the finite fields and rings is examined first, and detailed methods for determining them are discussed. Using standard results in group theory [22-29], the results for the cyclic classes of systems are then extended to general classes of these categories of P-I systems and their characterizations in terms of generalized finite discrete transforms are obtained. It is observed that the FDT defined by the cyclic class of P-I systems may be used with appropriate choices of the modulus of the ring, to obtain the familiar types of the so-called number-theoretic transforms (NTT's).

Finally in Chapter 8, a summary of the results presented in this thesis is given along with suggestions for further work.

1.3 Terminology and Notation

In this section we explain the terminology and notation used in this thesis.

Z_k, where k is some arbitrary positive interger, denotes the set of all non-negative integers less than k. Thus, $Z_k = \{0,1,2,\ldots,k-1\}$.

V denotes the signal space of 2-D P-I systems and is the vector space of real m x n matrices, where m and n are some arbitrary positive integers. Its dimension is N = m.n.

The set $\Delta_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$, of N matrices, where each $\Delta_{i,j}$ is an m x n matrix with a 1 in the i,j-th position and zeros everywhere else, denotes a basis set, called the standard basis set, for the space V.

R^N represents the vector space of real N-tuples and the set of N vectors e_i, $i\varepsilon Z_N$, where each e_i is a column vector of length N with a 1 in the i-th place and zeros everywhere else, forms a basis set, called the standard basis set, for the space R^N.

The upper case letter X is in general used to denote the FDT of a signal represented by the lower case letter x, where x may be either a 1-D signal or a 2-D signal, as specified in any particular context. However, in Chapter 3, in dealing with the equivalence between 2-D and 1-D P-I systems, it has been found convenient to use the upper case letter X to denote a 2-D signal belonging to V and the lower letter x to denote a 1-D signal belonging to R^N.

CHAPTER 2

2-D PERMUTATION-INVARIANT LINEAR SYSTEMS

2-D P-I systems form a subset of a broader class of systems called 2-D finite discrete linear systems. We begin in section 2.1 with a brief study of this broader class of systems and the associated signal space. In section 2.2 we introduce the notion of permutation-invariance in two dimensions and later give a formal definition of 2-D P-I systems using as a guideline, the notion of 1-D P-I systems introduced earlier [1] . Characterization of 2-D P-I systems in terms of their unit response matrices and system eigenvectors forms the contents of the remaining sections of this chapter.

2.1 Finite Discrete 2-D Signals and Systems

A finite discrete 2-D signal is a matrix or a double-indexed array of numbers with each one of the indices running

over a finite index set. When viewed in this manner, a 2-D signal is essentially a function $f: Z_m \times Z_n \rightarrow R$, where m and n are arbitrary positive integers, Z_k is the index set consisting of the integers $0, 1, \cdots, (k-1)$, and R denotes the real line. With the usual componentwise addition and scalar multiplication by reals, the totality of 2-D signals constitute the vector space V of real m x n matrices. This space has dimension m.n and the matrices $\Delta_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$, where each $\Delta_{i,j}$ is an m x n matrix with a 1 in the (i,j)-th position and zeros everywhere else, constitute for it a basis, called the standard basis. This signal space will henceforth be denoted by V throughout the thesis.

By a 2-D finite discrete system we mean a system whose input and output signals are from V. Such a system T is thus a transformation $T: V \rightarrow V$, and if it is linear then it is completely characterized by the matrices

$$T_{i,j} \overset{d}{=} T(\Delta_{i,j}) \quad ; \quad i\varepsilon Z_m,\ j\varepsilon Z_n ,$$

which are referred to here as the standard response matrices. Indeed, following the usual arguments for linear transformations, we have for any input $x\varepsilon V$, the output y given by

$$y = Tx = T \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} \Delta_{i,j} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} T_{i,j}$$

This means that from a knowledge of the standard response matrices $T_{i,j}$'s, the output for any input x is completely determined.

Remark 2.1.1: By analogy with the unit impulse sequence or the unit sample sequence of the discrete LTI systems, the $m \times n$ matrix $\Delta_{0,0}$ with a 1 in the (0,0)-th position and zeros everywhere else, is taken here as the unit sample signal for the 2-D finite discrete linear systems.

2.2 2-D Permutation-Invariant Systems

A system whose input and output signals are of the form $x(t)$, $-\infty < t < +\infty$, is said to be time-invariant, if the consequence of shifting the input signal $x(t)$ on the time scale is to produce an exactly identical shift in the output signal. When dealing with finite discrete signals such as n-tuples of reals, the notion of time-invariance is replaced by the analogous notion of permutation-invariance. Thus, a 1-D finite discrete linear system T is defined (Appendix A) to be permutation-invariant relative to a transitive abelian permutation group G, if as a result of permuting its input signal by any member of G the output also gets permuted exactly in an identical manner.

A 2-D finite discrete signal $x \varepsilon V$ is an array with m rows and n columns. Inasmuch as a permutation is a rearrangement of the members of a finite set of discrete objects, we may regard the m rows and n columns of x as two such finite sets of discrete objects and so permute each of them independently. Let T be a 2-D finite discrete linear system on V. Suppose $x \varepsilon V$ is an arbitrary input signal to this system. Suppose further, that we permute the rows of x by members of a transitive abelian group of permutations G_1 of order m and the columns by another transitive abelian permutation group G_2 of order n. If the effect of all such permutations to the rows and columns of x is that in each case, the rows and columns of the output signal of the system T get permuted exactly in the same manner, then T is invariant to such permutations and in this sense we say T is a 2-D permutation-invariant (2-D P-I) system relative to the pair of transitive abelian permutation groups G_1 and G_2. To state this more concretely in terms of matrices, it is convenient to assume throughout that the same symbol denotes the permutation as well as the permutation matrix representing it. More specifically, if p is a permutation for the rows then p also denotes the m x m matrix that results from permuting by p the rows of the identity matrix of size m. Similarly, if q is a permutation for the columns, then q also denotes the n x n matrix that results from permuting by q the columns of the identity

matrix of size n. Thus, the result of applying $p\varepsilon G_1$, and $q\varepsilon G_2$ to $x\varepsilon V$, is to give the permuted version of x which is concretely described by the matrix pxq^T. A formal definition of 2-D P-I systems is then as follows:

Definition 2.2.1: Let T be a 2-D finite discrete linear system on V. Let G_1 of order m and G_2 of order n be transitive abelian groups of permutation matrices of sizes m and n respectively. If for every $x\varepsilon V$, every $p_k\varepsilon G_1$, $k\varepsilon Z_m$ and every $q_l\varepsilon G_2$, $l\varepsilon Z_n$,

$$T(p_k x) = p_k(Tx), \tag{2.2.1}$$

and

$$T(xq_l^T) = (Tx)q_l^T, \tag{2.2.2}$$

then, T is said to be a 2-D P-I system relative to G_1 and G_2. Further, the set of all such systems satisfying (2.2.1) and (2.2.2) is said to constitute a class of 2-D P-I systems relative to G_1 and G_2. If G_1 and G_2 are the same group G, then we simply speak of permutation-invariance relative to G.

Consider T, a 2-D P-I system on V relative to G_1 and G_2. Let

$$p_k x = \underline{x} \; ; \; x\varepsilon V, \; p_k\varepsilon G_1, \; k\varepsilon Z_m \, .$$

Then from equation (2.2.2), for any $q_l\varepsilon G_2$, $l\varepsilon Z_n$,

$$T(\underline{x}q_1^T) = (T\underline{x})q_1^T = (T(p_k x))q_1^T.$$

But, from equation (2.2.1),

$$T(p_k x) = p_k(Tx).$$

Therefore,

$$T(p_k x q_1^T) = T(\underline{x}q_1^T) = (T(p_k x))q_1^T = (p_k(Tx))q_1^T$$

$$= p_k(Tx)q_1^T.$$

Thus, if

$$Tx = y \tag{2.2.3}$$

then,

$$T(p_k x q_1^T) = p_k(Tx)q_1^T = p_k y q_1^T. \tag{2.2.4}$$

Equations (2.2.3) and (2.2.4) more compactly express the fact that the effect of permuting the rows of the input signal of a 2-D P-I system by members of G_1 and its columns by members of G_2 is to permute the rows and columns of the output signal exactly in the same manner.

Before proceeding with the study of 2-D P-I systems, we need to examine in detail, how a signal $x \varepsilon V$ gets altered when we permute its rows by members of G_1 and columns by members of G_2. This is done in the following section.

2.3 Mathematical Description of the Effect of Permuting a 2-D Signal

Let p_k, $k \varepsilon Z_m$, belong to G, a transitive abelian group of permutation matrices of order m. From the way the members of such a group are ordered (Appendix A) it is known that the effect of premultiplying a signal $x \varepsilon V$ by p_k is that the zeroth row of x gets shifted to the k-th row position. But how exactly the other rows get affected is not immediately clear. To clarify this let us first consider just an m-tuple of reals, $v = (v_0, v_1, ---, v_{m-1})^T$. Then it is known (Appendix A) that

$$p_k(v) = (v_{0 \ominus k}, v_{1 \ominus k}, v_{2 \ominus k}, ---, v_{m-1 \ominus k})^T, \tag{2.3.1}$$

i.e., the j-th element of $p_k(v)$ is given by

$$(p_k(v))_j = v_{j \ominus k} \quad ; \quad k, j \varepsilon Z_m, p_k \varepsilon G \quad , \tag{2.3.2}$$

where $\ominus$ denotes pointwise subtraction operation (Appendix A) in a mixed-radix number system with radices m_0, m_1, m_2, --- , m_{r-1} which are the invariants of the group G.

A 2-D finite discrete signal $x \varepsilon V$ is double indexed and of the form $x_{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$. When the rows and columns of x are being permuted independently by members of transitive abelian permutation groups G_1 and G_2 respectively, equation (2.3.2) can be directly applied independently to each one of the indices of the signal.

Let $x = \begin{bmatrix} x_{0,0} & x_{0,1} & \text{------} & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \text{------} & x_{1,n-1} \\ \vdots & \vdots & & \vdots \\ x_{m-1,0} & x_{m-1,1} & \text{----} & x_{m-1,n-1} \end{bmatrix}$

Then, $p_i(x) = \begin{bmatrix} x_{0 \ominus i,0} & x_{0 \ominus i,1} & \text{---} & x_{0 \ominus i,n-1} \\ x_{1 \ominus i,0} & x_{1 \ominus i,1} & \text{---} & x_{1 \ominus i,n-1} \\ \vdots & \vdots & & \vdots \\ x_{m-1 \ominus i,0} & x_{m-1 \ominus i,1} & \text{---} & x_{m-1 \ominus i,n-1} \end{bmatrix}$

Thus, the (k,l)-th element of $p_i(x)$ is given by

$$(p_i(x))_{k,l} = x_{k \ominus i,l} \quad ; \quad p_i \varepsilon G_1, i \varepsilon Z_m \,. \tag{2.3.3}$$

Also,

$$((x)q_j^T)_{k,l} = x_{k,l \boxminus j}, \; q_j \varepsilon G_2, \; j \varepsilon Z_n \,, \tag{2.3.4}$$

where, $\ominus$ denotes pointwise subtraction operation in a mixed-radix number system with mixed m_0, m_1, m_2, - - - , m_{r-1} which are the invariants of the group G_1, and $\boxminus$ denotes pointwise subtraction operation in the mixed-radix number system with mixed radices n_0, n_1, - - - , n_{s-1} which are the invariants of the group G_2.

Combining (2.3.3) and (2.3.4) we have,

$$(p_i \times q_j^T)_{k,l} = x_{k \ominus i,\ l \boxminus j} : \tag{2.3.5}$$

Equation (2.3.5) shows the precise way in which each element of the signal x is affected when its rows are permuted by members of G_1 and the columns are permuted by members of G_2. To be specific, it states that the k,l-th element of the signal obtained after permuting the rows and columns - rows by the i-th member of G_1 and columns by the j-th member of G_2, is the $(k \ominus i,\ l \boxminus j)$-th element of the original signal x. In the particular case when both G_1 and G_2 are cyclic, equation (2.3.5) becomes

$$(p_i \times q_j^T)_{k,l} = x_{(k-i)_m,\ (l-j)_n}, \tag{2.3.6}$$

where $(a-b)_c$ denotes subtraction modulo c.

To consolidate the above ideas, we shall now consider several examples. We first illustrate the mixed-radix system to clarify how the row or column indices are changed as a result of applying the permutations.

Example 2.3.1: For the mixed radices $m_0 = 4$ and $m_1 = 2$, the mixed-radix weights are $w_0 = 1$, $w_1 = 4$ and $w_2 = 4 \times 2 = 8$. Any number k in the range 0 to 7 can be expressed uniquely using these mixed radices in the form $k = w_1\alpha_1 + w_0\alpha_0$. In the positional notation k may then be written as $< \alpha_1, \alpha_0 >$.

Table 2.1: The Mixed-Radix Digits for Numbers 0 to 7

Number	Mixed-Radix Digits α_1	α_0
0	0	0
1	0	1
2	0	2
3	0	3
4	1	0
5	1	1
6	1	2
7	1	3

Pointwise subtraction of integers in the mixed-radix system that results from such a representation of numbers is carried out as follows:

If i and j are two integers in the usual representation with fixed radix = 10, then first find the mixed-radix representations for i and j. Let

$$i = \langle i_1, i_0 \rangle \text{ and } \quad j = \langle j_1, j_0 \rangle .$$

Then,

$$i \ominus j = \langle (i_1 - j_1)_2, (i_0 - j_0)_4 \rangle ,$$

where the suffixes 4 and 2 are the values of the radices m_0 and m_1 respectively.

Thus,

$$
\begin{aligned}
0 \ominus 2 &= \langle (0-0)_2,\ (0-2)_4 \rangle = \langle 0,2 \rangle = 2 \\
1 \ominus 2 &= \langle (0-0)_2,\ (1-2)_4 \rangle = \langle 0,3 \rangle = 3 \\
2 \ominus 2 &= \langle (0-0)_2,\ (2-2)_4 \rangle = \langle 0,0 \rangle = 0 \\
3 \ominus 2 &= \langle (0-0)_2,\ (3-2)_4 \rangle = \langle 0,1 \rangle = 1 \\
4 \ominus 2 &= \langle (1-0)_2,\ (0-2)_4 \rangle = \langle 1,2 \rangle = 6 \\
5 \ominus 2 &= \langle (1-0)_2,\ (1-2)_4 \rangle = \langle 1,3 \rangle = 7 \\
6 \ominus 2 &= \langle (1-0)_2,\ (2-2)_4 \rangle = \langle 1,0 \rangle = 4 \\
7 \ominus 2 &= \langle (1-0)_2,\ (3-2)_4 \rangle = \langle 1,1 \rangle = 5 .
\end{aligned}
$$

Example 2.3.2: Consider the signal x

$$
x = \begin{bmatrix}
x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} & x_{0,4} \\
x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\
x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\
x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} \\
x_{4,0} & x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} \\
x_{5,0} & x_{5,1} & x_{5,2} & x_{5,3} & x_{5,4} \\
x_{6,0} & x_{6,1} & x_{6,2} & x_{6,5} & x_{6,4} \\
x_{7,0} & x_{7,1} & x_{7,2} & x_{7,3} & x_{7,4}
\end{bmatrix} .
$$

Let G_1 be the transitive abelian permutation group isomorphic to the abstract group with invariants 4 and 2 and let G_2 be the transitive abelian permutation group isomorphic to the abstract cyclic group of order 5. For G_1 we have

$m_0 = 2^3$ and $m_1 = 2$ and $m_0 = 5$ for G_2. We will now determine $(p_2 \times q_4^T)$, i.e., the signal obtained by permuting the rows of x by $p_2 \varepsilon G_1$ and the columns by $q_4 \varepsilon G_2$.

By using the results of the previous example, the permuted signal may be written as

$$(p_2 \times q_4^T) = \begin{bmatrix} x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} & x_{2,0} \\ x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} & x_{3,0} \\ x_{0,1} & x_{0,2} & x_{0,3} & x_{0,4} & x_{0,0} \\ x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} & x_{1,0} \\ x_{6,1} & x_{6,2} & x_{6,3} & x_{6,4} & x_{6,0} \\ x_{7,1} & x_{7,2} & x_{7,3} & x_{7,4} & x_{7,0} \\ x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} & x_{4,0} \\ x_{5,1} & x_{5,2} & x_{5,3} & x_{5,4} & x_{5,0} \end{bmatrix}.$$

2.4 Characterization of 2-D P-I Systems - The Unit Response Matrix

As mentioned in section 2.1, a finite discrete linear 2-D system T is completely characterized by its standard response matrices

$$T_{i,j} \stackrel{d}{=} T(\Delta_{i,j}) \quad ; \quad i \varepsilon Z_m, \; j \varepsilon Z_n .$$

2-D P-I systems are finite discrete linear 2-D systems endowed with the special property of permutation invariance as defined

in section 2.2. We shall now see how this property of permutation invariance permits a simplified characterization of these systems. Consider a 2-D P-I system T defined relative to G_1 and G_2. For any p_i and q_j, $i \varepsilon Z_m$, $j \varepsilon Z_n$, $p_i \varepsilon G_1$ and $q_j \varepsilon G_2$, we first observe that

$$p_i \, \Delta_{0,j} = \Delta_{i,j} \text{ and } \Delta_{i,0} \, q_j^T = \Delta_{i,j} ,$$

so that,

$$\Delta_{i,j} = p_i \Delta_{0,j} = p_i \Delta_{0,0} \, q_j^T .$$

Then, since T is a 2-D P-I system defined relative to G_1 and G_2, we have

$$T_{i,j} = T \Delta_{i,j} = T(p_i \, \Delta_{0,0} \, q_j^T) = p_i(T(\Delta_{0,0} \, q_j^T))$$

$$= p_i(T \, \Delta_{0,0}) \, q_j^T = p_i \, T_{0,0} \, q_j^T .$$

Hence the standard response matrices $T_{i,j}$ satisfy the relationship

$$T_{i,j} = p_i \, T_{0,0} \, q_j^T .$$

This is summarized in the following theorem:

Theorem 2.4.1: Let T be a 2-D P-I system relative to G_1 and G_2. Then its standard response matrices are obtained from $T_{0,0}$, the first of these matrices, by permuting its rows by

members of G_1 and its columns by members of G_2, i.e.,

$$T_{i,j} = p_i\ T_{0,0}\ q_j^T \quad ; \quad i \varepsilon Z_m,\ j \varepsilon Z_n,\ p_i \varepsilon G_1,\ q_j \varepsilon G_2 \,. \tag{2.4.1}$$

Thus, a knowledge of $T_{0,0}$, which is the system response to the unit sample signal $\Delta_{0,0}$, completely characterizes the system T.

In view of this result, $T_{0,0}$ plays the same important role that the impulse response ~~has~~ does in the case of time-invariant systems and so we give it a special status.

Definition 2.4.1: $T_{0,0}$, the first of the standard response matrices of a 2-D P-I system will be referred to as the unit response of the system.

Theorem 2.4.1 suggests the existence of a very convenient output-input relationship for these systems in terms of the unit response matrix, say s, and the defining groups G_1 and G_2. This takes us to the generalized convolutional relationship which will be derived in what follows.

2.4.1 The Generalized Convolutional Relationship for 2-D P-I Systems

Let T be a 2-D P-I system relative to G_1 and G_2. Using equations (2.3.5) and (2.4.1) we may write down the expression for the k,l-th element of the standard response

matrix $T_{i,j}$ of T as

$$(T_{i,j})_{k,l} = s_{k \ominus i, l \boxminus j} \; ; \quad k,i \varepsilon Z_m \; ; \; l,j \varepsilon Z_n \, , \qquad (2.4.2)$$

where as stated earlier, $\ominus$ denotes pointwise subtraction operation in the mixed-radix system of representation of numbers with mixed radices m_o, m_1, - - - , m_{r-1} that are the invariants of G_1, and $\boxminus$ denotes a similar operation but with the difference that in this case the mixed radices are n_o, n_1, - - - , n_{s-1} which are the invariants of group G_2.

Let $x \varepsilon V$ be any arbitrary 2-D signal. Then

$$y = Tx = T \sum_{i=o}^{m-1} \sum_{j=o}^{n-1} x_{i,j} \Delta_{i,j}$$

$$= \sum_{i=o}^{m-1} \sum_{j=o}^{n-1} x_{i,j} T(\Delta_{i,j})$$

$$= \sum_{i=o}^{m-1} \sum_{j=o}^{n-1} x_{i,j} T_{i,j} \, .$$

Using equation (2.4.2) we next get

$$y_{k,l} = \sum_{i=o}^{m-1} \sum_{j=o}^{n-1} s_{k \ominus i, l \boxminus j} \, x_{i,j} \, .$$

Here, $s_{k,l}$ is the (k,l)-th entry of the unit response matrix s of the system T. This equation will be called the generalized convolutional relationship that relates the

output and input for the class of 2-D P-I systems defined relative to G_1 and G_2.

Theorem 2.4.2: A 2-D P-I system T relative to G_1 and G_2 is characterized by the generalized convolutional relationship

$$y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{k \ominus i, l \boxminus j}\, x_{i,j} \quad ;$$

$$k \varepsilon Z_m, \; l \varepsilon Z_n \; , \qquad (2.4.3)$$

where x,y, and s are respectively the input, output and system's unit response arrays ; $\ominus$ and $\boxminus$ respectively denote pointwise subtraction operation in two mixed-radix number systems, one with radices m_o, m_1, - - -, m_{r-1} that are the invariants of G_1 and the other with radices n_o, n_1, - - - , n_{s-1} that are the invariants of G_2.

2.5 The Vector Space of a Class of 2-D P-I Systems

It was shown in the ~~last~~ previous section that each class of 2-D P-I systems has a convolutional characterization given by (2.4.3). In this section we shall show that each class of 2-D P-I systems forms a vector space. We will then determine the dimension of this vector space and choose an appropriate basis for it.

Let S denote the class of 2-D P-I systems defined relative to G_1 and G_2. Then for $p_k \varepsilon G_1$, $k \varepsilon Z_m$; $q_l \varepsilon G_2$, $l \varepsilon Z_n$, and T, RεS,

$$(T + R)(p_k x) = T(p_k x) + R(p_k x) .$$

But since T , RεS,

$$T(p_k x) = p_k(Tx) \text{ and } R(p_k x) = p_k(Rx) .$$

Therefore,

$$(T + R)(p_k x) = T(p_k x) + R(p_k x) = p_k(Tx) + p_k(Rx)$$

$$= p_k((T + R)x).$$

Also,

$$(T + R)(xq_l^T) = T(xq_l^T) + R(xq_l^T) = (Tx)q_l^T + (Rx)q_l^T$$

$$= (Tx + Rx)q_l^T = ((T + R)x)q_l^T .$$

Thus, if T , RεS then

$$(T + R)(p_k x) = p_k((T + R)x),$$

and

$$(T + R)(xq_l^T) = ((T + R)x)q_l^T .$$

Therefore,

$$(T + R)\varepsilon S .$$

Further, for any scalar α belonging to the real line,

$$\alpha T(p_k x) = \alpha(p_k(Tx)) = \alpha p_k(Tx) = p_k \alpha(Tx) = p_k(\alpha Tx).$$

Also,

$$\alpha T(xq_1^T) = \alpha((Tx)q_1^T) = (\alpha Tx)q_1^T ,$$

i.e., $\alpha T \varepsilon S$

Closed under addition and scalar multiplication, S is thus a vector space.

Theorem 2.5.1: A class of 2-D P-I systems, i.e., the set of all 2-D P-I systems relative to a pair of groups G_1 and G_2, forms a vector space over R, the real field.

The members of a class, say S, are also closed under composition, which may be treated as the binary operation of multiplication over the set S. Specifically,

$$RT(p_k x) = R(p_k(Tx)) = p_k(R(Tx)) = p_k(RT(x)).$$

Also,

$$RT(xq_1^T) = R((Tx)q_1^T) = (R(Tx)q_1^T) = (RT(x)q_1^T).$$

Therefore, if $R, T \varepsilon S$, then $RT \varepsilon S$.

This means that S can be treated as an algebra. However, for the present purposes we shall treat it just as a vector space, occasionally making use of its multiplicative closure to facilitate analysis.

2.5.1 A Basis for S

Now, to determine the dimension of S treated as a vector space and also to choose a suitable basis for it, let s be the unit response matrix of a 2-D P-I system T belonging to the class S. Then using the generalized convolutional relationship, the k,l-th element of the output may be written as

$$y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{k \ominus i,\, l \boxminus j}\, x_{i,j}\,,$$

where $s_{k,l}$ is the k,l-th entry in the unit sample response s of the system T.

Putting $k \ominus i = p$ and $l \boxminus j = q$,

$$y_{k,l} = \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} s_{p,q}\, x_{k \ominus p,\, l \boxminus q}\,.$$

Therefore,

$$y = \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} y_{k,l}\, \Delta_{k,l}$$

$$= \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} \left[\sum_{p=0}^{m-1} \sum_{q=0}^{n-1} s_{p,q}\, x_{k \ominus p,\, l \boxminus q} \right] \Delta_{k,l}$$

$$= \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} s_{p,q} \left[\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} x_{k \ominus p,\, l \boxminus q}\, \Delta_{k,l} \right].$$

But from equation (2.3.5) we have,

$$x_{k \ominus p,\, l \boxminus q} = (p_p \times q_q^T)_{k,l} \quad ; \quad p_p \varepsilon G_1, p \varepsilon Z_m \; ;$$

$$q_q \varepsilon G_2, q \varepsilon Z_n .$$

Therefore,

$$y = Tx = \sum_{p=o}^{m-1} \sum_{q=o}^{n-1} s_{p,q} \sum_{k=o}^{m-1} \sum_{l=o}^{n-1} (p_p \times q_q^T)_{k,l} \Delta_{k,l}$$

$$= \sum_{p=o}^{m-1} \sum_{q=o}^{n-1} s_{p,q} (p_p \times q_q^T).$$

Defining systems $B_{i,j}, i \varepsilon Z_m, j \varepsilon Z_n$, by the relation

$$B_{i,j}\, x \overset{d}{=} p_i \times q_j^T \quad \text{for} \quad x \varepsilon V, p_i \varepsilon G_1, q_j \varepsilon G_2 \tag{2.5.1}$$

we may write,

$$y = Tx = \left(\sum_{i=o}^{m-1} \sum_{j=o}^{n-1} s_{i,j}\, B_{i,j} \right) x . \tag{2.5.2}$$

Therefore,

$$T = \sum_{i=o}^{m-1} \sum_{j=o}^{n-1} s_{i,j}\, B_{i,j} . \tag{2.5.3}$$

Thus, any system $T \varepsilon S$ may be written down as a linear combination of the members of the set $B_{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$.

We shall now show that $B_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$, are linearly independent.

Suppose, $B_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$, are not linearly independent. Then there exists a set of coefficients $a_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ not all zero, such that

$$\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} B_{i,j}\right) x = 0, \text{ for every } x\varepsilon V ,$$

$$\text{i.e., } \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}\, p_i\, x\, q_j^T = \Theta \quad , \text{ for every } x\varepsilon V .$$

Since the above equation is true for every $x\varepsilon V$, let us put $x = \Delta_{0,0}$. Then we have,

$$\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} B_{i,j}\right)x = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}\, p_i\, \Delta_{0,0}\, q_j^T$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}\, \Delta_{i,j} = \emptyset .$$

But $\displaystyle\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j}\, \Delta_{i,j} = 0$ implies that

$$a_{i,j} = \theta \quad \text{for every } i\varepsilon Z_m \text{ and every } j\varepsilon Z_n.$$

This contradicts our earlier assumption about the $a_{i,j}$'s that not all of them are zero. Hence, $B_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ are

linearly independent and according to (2.5.3) they span the space S. Thus, the operators or transformations $B_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ defined by the formulae (2.5.1) constitute a basis set for the space S of the class of 2-D P-I systems defined relative to G_1 and G_2. So, the dimension of the space S is m.n. Thus, the following theorem is fully established:

Theorem 2.5.2: Let S be a class of P-I systems defined relative to G_1 of order m and G_2 of order n, and whose input and output signals belong to V, the space of real m x n matrices. Then S is a vector space of dimension m.n over the real field. Further, the systems $B_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ defined by formulae (2.5.1) constitute a basis for S, i.e., they are linearly independent and any system $T\varepsilon S$ is expressible as

$$T = \sum_{i=o}^{m-1} \sum_{j=o}^{n-1} s_{i,j}\, B_{i,j}, \tag{2.5.4}$$

where $s_{i,j}$ are the entries of the unit response matrix, s, of the system T.

2.5.2 Properties of the Basis Set $B_{i,j}$

Property PR1: Elements of the basis set are closed under 'multiplication', i.e., under composition.

Proof: Let $B_{i,j}$ and $B_{k,l}$ be any two arbitrary members of the set $B_{i,j}$, $i,k\varepsilon Z_m$; $j,l\varepsilon Z_n$, and let x be an arbitrary signal. Then,

$$B_{i,j}(B_{k,l}(x)) = B_{i,j}(p_k \ x \ q_l^T) = p_i(p_k \ x \ q_l^T)q_j^T$$

$$= p_i p_k \ x \ q_l^T \ q_j^T = (p_i p_k)x(q_j q_l)^T.$$

The permutations p_i and p_k are members of the group G_1 so that

$$p_i p_k = p_p; p\varepsilon Z_m \text{ and } p_p \varepsilon G_1.$$

Similarly

$$q_j q_l = q_q; q\varepsilon Z_n, q_q \varepsilon G_2 .$$

Thus,

$$B_{i,j}(B_{k,l}x) = p_p \ x \ q_q^T = B_{p,q}x .$$

Hence the set $B_{i,j}$ is closed under multiplication.

Property PR2: Elements of the basis set $B_{i,j}$ are pairwise commutative.

Proof: $B_{i,j}(B_{k,l}(x)) = B_{i,j}(p_k \ x \ q_l^T) = p_i p_k \ x \ q_l^T \ q_j^T$

Since p_i and p_k are members of the abelian multiplicative group G_1 they commute. Similarly q_l and q_j also commute. Hence,

$$B_{i,j}(B_{k,l}(x)) = p_i p_k \ x \ q_l^T \ q_j^T = p_k p_i \ x \ q_j^T \ q_l^T$$

$$= p_k(p_i \ x \ q_j^T)q_l^T = B_{k,l}(B_{i,j}(x)),$$

i.e., $B_{i,j} \ B_{k,l}(x) = B_{k,l} \ B_{i,j}(x)$, for every $x\varepsilon V$.

Therefore,

$$B_{i,j} \cdot B_{k,l} = B_{k,l} \cdot B_{i,j}, \text{ for every } i,k \varepsilon Z_m \text{ and every } j,l \varepsilon Z_n .$$

Thus the elements of the basis set $B_{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$ are pair-wise commutative.

An immediate consequence of the above properties of the systems $B_{i,j}$ is that any two members of a class of 2-D P-I systems commute. More formally,

Theorem 2.5.3: If T and R are two 2-D P-I systems of the same class, then $TRx = RTx$ for every 2-D signal $x \varepsilon V$.

Proof: From (2.5.3) we may write

$$T = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} B_{i,j} ,$$

where s is the unit response matrix of T.

Also,

$$R = \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} r_{k,l} B_{k,l}$$

where r is the unit response matrix of R. Let x be any arbitrary 2-D signal in V. Then,

$$TR(x) = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} B_{i,j} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} r_{k,l} B_{k,l} \right) x$$

$$= \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} r_{k,l} B_{i,j} B_{k,l} \right) x$$

$$= \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} r_{k,l} B_{k,l} B_{i,j} \right) x$$

$$= \left(\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} r_{k,l} B_{k,l} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} B_{i,j} \right) x = RT(x)$$

which completes the proof of this theorem.

Now let us consider V as an inner product space by choosing a suitable inner product on it. For this choice consider the pointwise product, C, of two m x n matrices A and B, also sometimes called their Schur product, written as $C = A \circ B$, which is defined by the relation

$$C_{i,j} = A_{i,j} \cdot B_{i,j} \quad ; \quad i \varepsilon Z_m, \ j \varepsilon Z_n.$$

With any appropriate norm $\| \cdot \|$ for the space V, we then choose for the inner product on V,

$$(x,y) = \| x \circ y \|^2 \quad ; \quad x,y \varepsilon V.$$

For definiteness, the norm used is Euclidean,

$$\| x \| = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j}^2 \right)^{\frac{1}{2}}.$$

We now treat V as an inner product space of dimension m.n and show that $B_{i,j}$ is a normal operator [30, p. 312] on it. We first note that

$$(B_{i,j}x) \circ y = (p_i \, x \, q_j^T) \circ y = x \circ (p_i^{-1} \, y (q_j^{-1})^T)$$

$$= x \circ (p_i^T \, y \, q_j) = x \circ (B_{i,j}^* \, y),$$

Thus, $(B_{i,j}x) \circ y = x \circ (B_{i,j}^* y)$, (2.5.5)

Where $B_{i,j}^*$ is the system defined by

$$B_{i,j}^* x = p_i^T \, x \, q_j \qquad ; \qquad \text{for every } x \varepsilon V. \tag{2.5.6}$$

Since $(B_{i,j}x, y) = || (B_{i,j}x) \circ y ||^2$, from equation (2.5.5) we have

$$(B_{i,j}x, y) = || (B_{i,j}x) \circ y ||^2 = || x \circ (B_{i,j}^* y) ||^2$$

$$= (x, B_{i,j}^* y).$$

Thus $B_{i,j}^*$ defined as in equation (2.5.6), is the adjoint of $B_{i,j}$.

Further, we have

$$B_{i,j} \, B_{i,j}^* x = p_i (p_i^T \, x \, q_j) q_j^T = x = p_i^T (p_i \, x \, q_j^T) q_j$$

$$= B_{i,j}^* \, B_{i,j} \, x \text{ for every } x \varepsilon V.$$

This shows that $B_{i,j}$ commutes with its adjoint, i.e., $B_{i,j}$ is a normal operator on V for any $i\varepsilon Z_m$ and any $j\varepsilon Z_n$. From property PR2 we already know that the systems $B_{i,j}$ are pairwise commutative. Thus,

Theorem 2.5.4: If S is a class of 2-D P-I systems then the pairwise commutative systems $B_{i,j}$ defined by equation (2.5.1) which form a basis for S are normal operators on V, the signal space for S.

That $B_{i,j}$ are commutative normal operators on V is a useful property in that, it allows us to directly make use of the spectral theory of normal operators [30,31] to arrive at the eigenvectors of the systems $B_{i,j}$ and the class S of 2-D P-I systems for which they serve as a basis.

2.6 Eigenvalues and Eigenvectors of 2-D P-I Systems

In the ~~last~~ previous section we had seen that the systems $B_{i,j}$ form a basis for the vector space S of a class of 2-D P-I systems. Further, by virtue of property PR3, they are a set of commutative normal operators on V, the space of real m x n matrices.

But then, it is known [30,31] that the members of a set of normal operators on a finite-dimensional inner-product space V have in common a set of orthonormal eigenvectors iff

the operators are pairwise commutative. It has already been shown that the systems $B_{i,j}$ are pairwise commutative normal operators on the inner product space V. Hence, the set of basis systems $B_{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$, have a common set of m.n orthonormal eigenvectors that span the space V. Since any member of S can be expressed as a linear combination of the systems $B_{i,j}$, it then follows that all the members of S, a class of 2-D P-I systems on V, have a common set of orthonormal eigenvectors that span the space V. Thus, we have fully established the following theorem:

Theorem 2.6.1: All members of S, a class of P-I systems defined on V, the space of real m x n matrices, have a common set of m.n orthonormal eigenvectors that span the space V.

We now proceed to determine these eigenvectors. For this purpose, however, it would be more expedient to establish a relationship between the eigenvectors of the class S of 2-D P-I systems relative to groups G_1 and G_2 on the one hand, and those of the classes of 1-D P-I systems S_1 and S_2 on the other, where, S_1 is the class of 1-D P-I system relative to G_1 and S_2, the class relative to G_2. Before proceeding with this task, we would like to make the following remark:

Remark 2.6.1: Since the real number field is not algebraically closed, for the purpose of dealing with the eigenvalues

and eigenvectors of 2-D P-I systems we shall take the signal space to be W, the space of complex m x n matrices ~~rather~~ rather than V, the space of real m x n matrices.

Let S_1 be a class of 1-D P-I systems relative to G_1. Then it is known that (Appendix A) $\{p_i \varepsilon G_1, i\varepsilon Z_m\}$ is ~~are~~ a basis for the vector space formed by S_1 and that all the members of the class S_1 have a common set of orthonormal eigenvectors. These eigenvectors given by $h_m^i, i\varepsilon Z_m$, span C^m, the space of complex m-tuples.

Further, let S_2 be a class of 1-D P-I systems relative to G_2. Then $q_j \varepsilon G_2$, $j\varepsilon Z_n$, provide a basis for the vector space formed by S_2 and all members of S_2 have a common set of orthonormal eigenvectors given by h_n^j, $j\varepsilon Z_n$, which span C^n.

Now consider S, the class of 2-D P-I systems on W relative to G_1 and G_2. Then, referring to theorem 2.5.1, the systems $B_{k,l}$, $k\varepsilon Z_m$, $l\varepsilon Z_n$, defined by equation 2.5.1, form a basis for S, and all the members of S have a common set of orthonormal eigenvectors that span the space W.

Now, to see the relationship between the eigenvectors of S and those of S_1 and S_2, let h_m^i be the i-th eigenvector of the systems belonging to S_1, and h_n^j be the j-th eigenvector of the systems belonging to S_2. Then, it is known (Appendix A) that the k-th entry, $k\varepsilon Z_n$, of h_n^j is given by

$$h_n^{k,j} = \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{k_\alpha j_\alpha} \quad ; \quad k, j\varepsilon Z_n \quad , \tag{2.6.1}$$

where k_α and j_α, $\alpha \varepsilon Z_r$ are the mixed-radix digits in the expansion of k and j respectively with respect to the mixed radices m_α, $\alpha \varepsilon Z_r$ which are the invariants of G_2, and γ_{m_α} is the m_α-th root of unity given by

$$\gamma_{m_\alpha} = \exp(\sqrt{-1}\, \frac{2\pi}{m_\alpha}), \quad \alpha \varepsilon Z_r \,. \tag{2.6.2}$$

Further,

$$p_k\, h_m^i = \sigma_m^{i,k}\, h_m^i = \bar{h}_m^{i,k}\, h_m^i \quad ; \quad p_k \varepsilon G_1 \,, \tag{2.6.3}$$

and

$$q_l\, h_n^j = \sigma_n^{j,l}\, h_n^j = \bar{h}_n^{j,l}\, h_n^j \quad ; \quad q_l \varepsilon G_2 \,, \tag{2.6.4}$$

where $\sigma_m^{i,k}$ is the i-th eigenvalue of the matrix $p_k \varepsilon G_1$, the eigenvector associated with this eigenvalue being h_m^i and $\sigma_n^{j,l}$ is the j-th eigenvalue of the matrix $q_l \varepsilon G_2$, the eigenvector associated with this eigenvalue being h_n^j. Further, $\bar{h}_m^{i,k}$ is the complex conjugate of $h_m^{i,k}$ defined as in equation (2.6.1).

Now define $h_N^{i,j}$ as

$$h_N^{i,j} = h_m^i \,.\, (h_n^j)^T \quad ; \quad i \varepsilon Z_m,\ j \varepsilon Z_n . \tag{2.6.5}$$

If 2-D P-I systems $B_{k,l}$, $k \varepsilon Z_m$, $l \varepsilon Z_n$ defined as in equation (2.5.1) are considered, then

$$\begin{aligned} B_{k,l}\, h_N^{i,j} &= p_k\, h_N^{i,j}\, q_l^T = p_k\, h_m^i\, (h_n^j)^T\, q_l^T \\ &= (p_k\, h_m^i) \cdot (q_l\, h_n^j)^T = \sigma_m^{i,k}\, \sigma_n^{j,l} .\, h_m^i\, (h_n^j)^T \\ &= \sigma_m^{i,k} .\, \sigma_n^{j,l} .\, h_N^{i,j} \,, \end{aligned}$$

i.e., $B_{k,l}\, h_N^{i,j} = \sigma_m^{i,k} \cdot \sigma_n^{j,l}\, h_N^{i,j}$. (2.6.6)

Thus, $h_N^{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ defined by equation 2.6.5, are the eigenvectors of the basic 2-D P-I systems $B_{k,l}$, $k\varepsilon Z_m$, $l\varepsilon Z_n$ of the class S. Since any system $T\varepsilon S$ is a linear combination of the basic systems $B_{k,l}$ of that class, it follows that all members of S have a common set of orthonormal eigenvectors $h_N^{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$. Specifically, if $T\varepsilon S$ is given by (equation 2.5.3)

$$T = \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\, B_{k,l}\,, \tag{2.6.7}$$

where $s_{k,l}$, $k\varepsilon Z_m$, $l\varepsilon Z_n$ are the entries of the unit response matrix s of T. Then referring to equation (2.6.6),

$$\begin{aligned} Th_N^{i,j} &= \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\, B_{k,l}\, h_N^{i,j} \\ &= \left(\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\, \sigma_m^{i,k}\, \sigma_n^{j,l}\right) h_N^{i,j} \quad ; \end{aligned}$$

$$\text{for every } i\varepsilon Z_m, \text{ every } j\varepsilon Z_n. \tag{2.6.8}$$

Thus, the (i,j)-th eigenvector $h_N^{i,j}$ of a 2-D P-I system T belonging to S is associated with the (i,j)-th eigenvalue given by

$$\sigma_T^{i,j} = \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\, \sigma_m^{i,k}\, \sigma_n^{j,l} \quad ; \quad i\varepsilon Z_m,\ j\varepsilon Z_n\,, \tag{2.6.9}$$

where $\sigma_m^{i,k}$ and $\sigma_n^{j,l}$ are as defined in equations (2.6.3) and (2.6.4) respectively. We now summarize these results in the following theorem:

Theorem 2.6.2: Let S be a class of 2-D P-I systems relative to G_1 of order m and G_2 of order n. Let S_1 and S_2 be classes of 1-D P-I systems relative to G_1 and G_2 respectively. Then the (i,j)-th eigenvector $h_N^{i,j}$ of S is given by

$$h_N^{i,j} = (h_m^i)(h_n^j)^T \quad ; \quad i\varepsilon Z_m,\ j\varepsilon Z_n ,$$

where h_m^i and h_n^j are respectively the i-th eigenvector of S_1 and the j-th eigenvector of S_2. Further, if any $T\varepsilon S$ has a unit response matrix s, then the eigenvector $h_N^{i,j}$ of T is associated with the eigenvalue $\sigma_T^{i,j}$ given by

$$\sigma_T^{i,j} = \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\ \sigma_m^{i,k}\ \sigma_n^{j,l} \quad ; \quad i\varepsilon Z_m,\ j\varepsilon Z_n ,$$

where $\sigma_m^{i,k}$ is the i-th eigenvalue of the k-th permutation matrix $p_k\varepsilon G_1$ and $\sigma_n^{j,l}$ is the j-th eigenvalue of the l-th permutation matrix $q_l\varepsilon G_2$.

CHAPTER 3

EQUIVALENT 1-D SYSTEMS FOR 2-D P-I SYSTEMS

In Chapter 2, we defined a 2-D permutation-invariant system as a 2-D finite discrete linear system which exhibits invariance to permutations of the rows and columns of its input signal, where the permutations applied to the rows and columns separately form transitive abelian groups. In the present chapter, we establish an equivalence between members of a given class of 2-D P-I systems and those of a 'corresponding class' of 1-D P-I systems. This is done in the following three stages: In section 1, we deal with the problem of representing a given 2-D signal as an equivalent 1-D signal. This problem is viewed as one of establishing an isomorphism between V, the space of all real m x n matrices, and R^N, the space of all real N-tuples, $N = m.n$, through convenient linear transformations from V to R^N, which may be described in terms of suitable index mappings $f: Z_m \times Z_n \to Z_N$. We then show

in section 2 that permuting the rows and columns of $X \varepsilon V$ by members of G_1 and G_2 respectively is equivalent to permuting the equivalent 1-D signal $x \varepsilon R^N$ by the 'corresponding members' of another transitive abelian group G of permutation matrices, which is shown to be isomorphic to the direct product group $G_1 \times G_2$. Finally, in section 3, starting from a 2-D P-I system T on V defined relative to G_1 and G_2, we show that the equivalent 1-D finite discrete linear system t on R^N, obtained through a linear transformation Q from V to R^N, is indeed a permutation-invariant system relative to G.

The fact that a 2-D P-I system has associated with it an equivalent 1-D P-I system, gives rise to several interesting possibilities in the processing of 2-D data by 1-D techniques. The design of stable 2-D linear shift-invariant systems and digital filters is beset with problems of spectral factorization [8-12] that are not encountered in the 1-D case. Efforts to overcome these problems have led to elegant but somewhat cumbersome methods of 2-D facterization such as [11,12]. There have also been attempts to use 1-D techniques for 2-D tasks. McClellan [6] has proposed an algorithm which enables one to approximate many useful 2-D functions by converting an appropriate 1-D linear phase design into a linear phase 2-D design. In another approach [8] the unit sample response of a 1-D FIR filter designed to give the 1-D

ideal function which is obtained by appropriately slicing the given ideal 2-D function, is back-projected to give a 2-D unit sample response that was 'expected' to approximate the given 2-D ideal function. All these different methods are, however, limited in their efficacy by the fact [13] that an exact 1-D implementation of a 2-D linear shift-invariant filter does not possess the shift-invariance property. In contrast, as the results of this chapter show, a 2-D P-I filter or system which has the same role for finite discrete signals that the digital filters have for infinite sequences, has a 1-D implementation which is again permutation-invariant. In particular, if the original 2-D P-I system is of the cyclic kind, then with only a minor constraint on the frame size which does not in any way reduce its utility, one can design a 1-D cyclic P-I filter to perform the 2-D tasks, after an appropriate translation of the 2-D filter performance requirements into equivalent requirements on the 1-D filter (Chapter 6).

3.1 Representing 2-D Signals by 1-D Signals

As mentioned earlier, we will in this section seek some convenient methods of representing a 2-D finite discrete signal as a finite 1-D sequence.

The signal space for 2-D P-I systems is the vector space V of real matrices also called 2-D arrays or sequences of size m x n, where m and n are arbitrary positive integers; the dimension of V is $N = m.n$. Matrices $\Delta_{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$, each of size m x n, form the standard basis for V. An arbitrary 2-D signal $X \varepsilon V$ may then be written as

$$\begin{bmatrix} X_{0,0} & \cdots & X_{0,n-1} \\ \vdots & & \vdots \\ X_{m-1,0} & \cdots & X_{m-1,n-1} \end{bmatrix} ; \; X_{i,j} \varepsilon R, i \varepsilon Z_m, j \varepsilon Z_n \qquad (3.1.1)$$

A 'corresponding' 1-D finite discrete signal x on the other hand, is a single-indexed sequence of length $N = m.n$. The pertinent signal space for these is R^N, the space of all real N-tuples.

Clearly, a simple way of converting signals in V into corresponding or equivalent signals in R^N, is by defining a convenient linear transformation Q from V to R^N which simply rearranges the elements of a 2-D signal $X \varepsilon V$ into a 1-D sequence x of length N, i.e.,

$$Q : V \rightarrow R^N, \; x = Q(X) .$$

This transformation Q may be defined in terms of its effect on $\Delta_{i,j}$'s, the basis elements of V, by a mapping of the form,

$$Q(\Delta_{i,j}) = e_k \quad ; \quad i\varepsilon Z_m,\ j\varepsilon Z_n,\ k\varepsilon Z_N\ , \tag{3.1.2}$$

where e_k is a column vector of length N with a 1 in the k-th position and zeros everywhere else, i.e., e_k is the k-th member of the standard ordered basis set e_i, $i\varepsilon Z_N$, of R^N. Thus, under a transformation Q as defined by equation (3.1.2), a 2-D signal $X\varepsilon V$ will be transformed into a 1-D sequence $x\varepsilon R^N$, with the (i,j)-th element of X occupying the k-th position in x.

It is clear that a transformation of the type given by equation (3.1.2) may equivalently be described by a one-to-one index mapping f,

$$f : Z_m \times Z_n \rightarrow Z_N,\ N = m.n\ ,$$

i.e., in (3.1.2),

$$\left.\begin{array}{ll} & f(i,j) = k \\ \text{and} & f^{-1}(k) = (i,j) \end{array}\right\} . \tag{3.1.3}$$

Remark 3.1.1: The 1-D representation of X obtained through a transformation Q characterized by a mapping of the form (3.1.2) is a representation of X in terms of its coordinates relative to the basis matrices $\Delta_{i,j}$, when these are ordered according to the corresponding index mapping f of the form (3.1.3). We shall hereafter refer to f as the index mapping associated with the transformation Q.

Remark 3.1.2: If x is a 1-D signal given by

$$x = QX$$

where Q is a transformation of the form (3.1.2) and X is a 2-D signal, then x will be referred to as the 1-D equivalent of X.

A familiar example of an index mapping of the form (3.1.3) is provided by what is generally called the 'lexicographic ordering' of pairs of indices. Example 3.1.1 illustrates the use of this mapping for obtaining 1-D equivalent of a 2-D signal.

Example 3.1.1: $m = 2$, $n = 3$, $N = 2 \times 3 = 6$. Let the basis elements of V, viz., $\Delta_{i,j}$, $i\varepsilon Z_2$, $j\varepsilon Z_3$ be ordered lexicographically, i.e., according to the following index mapping f

$$k = f(i,j) = ni + j = 3i + j, \; i\varepsilon Z_2, \; j\varepsilon Z_3.$$

Let $$X = \begin{bmatrix} X_{0,0} & X_{0,1} & X_{0,2} \\ X_{1,0} & X_{1,1} & X_{1,2} \end{bmatrix}.$$

Then the resulting 1-D representation of X is the vector $x\varepsilon R^6$ given by $x = (X_{0,0}\; X_{0,1}\; X_{0,2}\; X_{1,0}\; X_{1,1}\; X_{1,2})^T$.

A less familiar but, nevertheless a very useful type of index mapping when m and n are relatively prime, is provided by

$$k = f(i,j) = (k_1 i + k_2 j) \bmod N \quad ; \quad i \varepsilon Z_m, j \varepsilon Z_n, N = m.n, \; k \varepsilon Z_N ,$$

where, k_1 and k_2 are appropriate integral multiples of n and m respectively. This mapping [32] has the interesting property of being cyclic with respect to all the three indices i, j and k, when k_1 and k_2 are properly chosen. We shall discuss this in detail in Chapter 6. For the present we consider the following example to illustrate its use for obtaining 1-D equivalent of a 2-D signal:

Example 3.1.2: m = 3, n = 5. Let $\Delta_{i,j}$, $i\varepsilon Z_3$, $j\varepsilon Z_5$ be ordered according to the mapping $k = f(i,j) = (10i + 6j) \bmod 15$; $i\varepsilon Z_3$, $j\varepsilon Z_5$, $k\varepsilon Z_{15}$.

$$\text{Let} \qquad X = \begin{bmatrix} X_{0,0} & X_{0,1} & X_{0,2} & X_{0,3} & X_{0,4} \\ X_{1,0} & X_{1,1} & X_{1,2} & X_{1,3} & X_{1,4} \\ X_{2,0} & X_{2,1} & X_{2,2} & X_{2,3} & X_{2,4} \end{bmatrix} .$$

The way the entries of the 2-D signal X are to be rearranged starting with $X_{0,0}$, in order to obtain the equivalent 1-D signal x, is indicated by the arrow-heads drawn in the array X.

Thus, the 1-D representation of X is given by $x\varepsilon R^{15}$, where

$$x = (X_{0,0}\ X_{1,1}\ X_{2,2}\ X_{0,3}\ X_{1,4}\ X_{2,0}\ X_{0,1}\ X_{1,2}\ X_{2,3}$$
$$X_{0,4}\ X_{1,0}\ X_{2,1}\ X_{0,2}\ X_{1,3}\ X_{2,4})^T.$$

Note that the linear transformation Q from V to R^N corresponding to this index mapping transforms the basis matrices $\Delta_{i,j}$ $i\varepsilon Z_m$, $j\varepsilon Z_n$, of V in the following manner:

$\Delta_{0,0}$	e_0	$\Delta_{1,2}$	e_7
$\Delta_{1,1}$	e_1	$\Delta_{2,3}$	e_8
$\Delta_{2,2}$	e_2	$\Delta_{0,4}$	e_9
$\Delta_{0,3}$	e_3	$\Delta_{1,0}$	e_{10}
$\Delta_{1,4}$	e_4	$\Delta_{2,1}$	e_{11}
$\Delta_{2,0}$	e_5	$\Delta_{0,2}$	e_{12}
$\Delta_{0,1}$	e_6	$\Delta_{1,3}$	e_{13}
		$\Delta_{2,4}$	e_{14}

where, e_k, $k\varepsilon Z_{15}$ is the standard ordered basis set of R^{15}.

Recall that the 2-D unit sample sequence is $\Delta_{0,0}$, an m x n matrix with a 1 in the (0,0)-th position and zeros everywhere else. Further, the 1-D unit sample sequence is e_0, the column vector with a 1 in the zeroth position and zeros everywhere else. In view of this, we make the following remark:

Remark 3.1.3: Although any one-to-one index mapping would serve the purpose, we shall utilize only those that map (0,0) to 0, since these mappings will cause the 2-D unit sample signal $\Delta_{0,0}$, to go into the 1-D unit sample sequence e_0. Incidentally, such mappings permit us to label members of the direct product group $G_1 \times G_2$ (remark 3.2.1) using the method adopted earlier in Chapter 2.

3.2 Equivalent Permutation on 1-D Signals

Having examined the question of representing any arbitrary 2-D signal $X \varepsilon V$ as a 1-D signal $x \varepsilon R^N$, logically the next step in our attempt to seek an equivalent 1-D system for any given 2-D P-I system would be to examine, what corresponding permutation the 1-D signal x undergoes, when the 2-D signal X has its rows and columns permuted by certain permutation matrices p_k and q_l respectively. To be more specific, consider the diagram of Fig. 3.1.

$$\begin{tikzcd}
V \arrow[r, "Q"] \arrow[d, "{p_k, q_l}"'] & R^N \arrow[d, "P_r"] \\
V \arrow[r, "Q"'] & R^N
\end{tikzcd}$$

Fig.3.1: Equivalent Permutation on 1-D Signals.

Let

i. X be an arbitrary 2-D signal,

ii. x be the 1-D representation of X under the linear transformation Q i.e., $x = QX$,

iii. p_k be an $m \times m$ permutation matrix acting on the rows of X and q_l an $n \times n$ permutation matrix acting on the columns of X,

iv. $X_p = p_k X q_l^T$, be the signal obtained after permuting the rows and columns of X, and

v. P_r be the matrix representation of the equivalent permutation on x such that if $x_p = P_r\, x$ then $X_p = Q^{-1} x_p$.

Now, the questions that arise are (a) what is the form of P_r ? (b) if $p_k \varepsilon G_1$ and $q_l \varepsilon G_2$ where G_1 and G_2 are transitive abelian groups of permutation matrices of orders m and n respectively, will the set P_r, $r \varepsilon Z_N$ of corresponding permutation matrices acting on x, constitute a transitive abelian group G ? (c) if the set P_r constitutes a transitive abelian group G of permutation matrices, how is the group G related to the groups G_1 and G_2 ?

Now since,

$$X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j} \, \Delta_{i,j} \; ,$$

$$x_p = Q(p_k X q_l^T) = Q(p_k(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j} \, \Delta_{i,j}) q_l^T)$$

$$Q(p_k \, \Delta_{i,j} q_l^T) = (p_k \delta_i) \otimes_Q (q_l \delta_j)$$

$$= (p_k \otimes_Q q_l)(\delta_i \otimes_Q \delta_j)$$

$$= (p_k \otimes_Q q_l) \; Q \; (\delta_i \; \delta_j^T)$$

$$= (p_k \otimes_Q q_l) \; Q \; (\; \Delta_{i,j}) \; ,$$

i.e., $Q(p_k \, \Delta_{i,j} q_l^T) = (p_k \otimes_Q q_l) \; Q \; (\; \Delta_{i,j}) .$

Using this in equation 3.2.1,

$$x_p = (\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} Q(p_k \; \Delta_{i,j} q_l^T) X_{i,j})$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (p_k \otimes_Q q_l) \; Q \; (\Delta_{i,j}) X_{i,j}$$

$$= (p_k \otimes_Q q_l) \; Q \; (\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \Delta_{i,j} \; X_{i,j})$$

$$= (p_k \otimes_Q q_l) \; Q \; (X) .$$

Since $x_p = Q(p_k \; X \; q_l^T)$, we have,

$$Q(p_k \; X \; q_l^T) = (p_k \otimes_Q q_l) \; Q \; (X) . \tag{3.2.4}$$

Equation (3.2.4) implies that, the permutation of rows of the 2-D signal X by p_k and columns by q_l is equivalent to the permutation of the 1-D representation x, of X by the N x N permutation matrix $(p_k \otimes_Q q_l)$.

The following examples illustrate these ideas:

Example 3.2.1:

$$X = \begin{bmatrix} X_{0,0} & X_{0,1} & X_{0,2} \\ X_{1,0} & X_{1,1} & X_{1,2} \end{bmatrix} \quad ; \quad m = 2,\ n = 3$$

Therefore, $N = m.n = 2.3 = 6$. Let the index mapping f associated with Q be given by

$$k = f(i,j) = 3i + j,\ i\varepsilon Z_m,\ j\varepsilon Z_n \text{ and } k\varepsilon Z_N .$$

This mapping corresponds to the lexicographic ordering of pairs of indices.

Let the rows of X be permuted by the matrix $p_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and the columns by $q_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

$$X_p = p_1\ X\ q_2^T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} X_{0,0} & X_{0,1} & X_{0,2} \\ X_{1,0} & X_{1,1} & X_{1,2} \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} X_{1,1} & X_{1,2} & X_{1,0} \\ X_{0,1} & X_{0,2} & X_{0,0} \end{bmatrix} .$$

Therefore,

$$Q(X_p) = x_p = (X_{1,1}\ X_{1,2}\ X_{1,0}\ X_{0,1}\ X_{0,2}\ X_{0,0})^T .$$

Also,

$$(p_1 \otimes_Q q_2) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} .$$

Therefore,

$$(p_1 \otimes_Q q_2)\ Q\ (X) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} X_{0,0} \\ X_{0,1} \\ X_{0,2} \\ X_{1,0} \\ X_{1,1} \\ X_{1,2} \end{bmatrix}$$

$$= (x_{1,1}\ x_{1,2}\ x_{1,0}\ x_{0,1}\ x_{0,2}\ x_{0,0})^T$$

$$= Q(p_1 \times q_2^T) .$$

Example 3.2.2: Consider the same 2-D signal as in the previous example, but let the index mapping associated with Q be

$$k = f(i,j) = (3i + 4j) \bmod 6,\ i\varepsilon Z_2,\ j\varepsilon Z_3,\ k\varepsilon Z_6 .$$

The mapping f is given in a tabular form in Table 3.1.

Table 3.1: Mapping of Indices in Example 3.2.2

(i,j)	k
0,0	0
1,1	1
0,2	2
1,0	3
0,1	4
1,2	5

Let the rows and columns of X be permuted by the same matrices as in the example 3.2.1.

$$X_p = p_1 \, X \, q_2^T = \begin{bmatrix} X_{1,1} & X_{1,2} & X_{1,0} \\ X_{0,1} & X_{0,2} & X_{0,0} \end{bmatrix}.$$

Therefore,

$$Q(X_p) = x_p = (X_{1,1} \;\; X_{0,2} \;\; X_{1,0} \;\; X_{0,1} \;\; X_{1,2} \;\; X_{0,0})^T.$$

While writing down the matrix form of $p_1 \otimes_Q q_2$, we note that the k-th column of $p_1 \otimes_Q q_2$ is obtained by taking $p_{1i} \otimes_Q q_{2j}$ where p_{1i} is the i-th column of p_1 and q_{2j} is the j-th column of q_2. Values of k corresponding to the particular values of i and j, $i \varepsilon Z_2$ and $j \varepsilon Z_3$, are obtained by using the index mapping f. Again, for writing down the elements of the k-th column of $p_1 \otimes_Q q_2$ in the proper order, we follow the index mapping, i.e., if a 1 occurs in the p-th place of p_{1i} and the q-th place of q_{2j} then a 1 occurs in the r-th place of the k-th column of $p_1 \otimes_Q q_2$, where the $r \varepsilon Z_6$ corresponding to (p,q) is obtained by using the index mapping.

Thus, $$p_1 \otimes_Q q_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

$$(p_1 \otimes_Q q_2)\, Q\,(x) = \begin{bmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0 \end{bmatrix} \begin{bmatrix} X_{0,0}\\ X_{1,1}\\ X_{0,2}\\ X_{1,0}\\ X_{0,1}\\ X_{1,2} \end{bmatrix}$$

$$= (X_{1,1}\; X_{0,2}\; X_{1,0}\; X_{0,1}\; X_{1,2}\; X_{0,0})^T = Q(p_1 \, X \, q_2^T).$$

Proceeding further, let the matrices p_k and q_l which permute respectively the rows and columns of the 2-D signal X, be members of transitive abelian groups of permutation matrices G_1 of degree and order m and G_2 of degree and order n, respectively. Then, we obtain a set M of N permutation matrices,

$$M \stackrel{d}{=} \{ p_k \otimes_Q q_l \} \quad , \; p_k \varepsilon G_1, \; q_l \varepsilon G_2 \; ; \; k \varepsilon Z_m, \; l \varepsilon Z_n$$

every member of which satisfies equation 3.2.4. We shall now show that this set M forms a transitive abelian group G of order N = m.n. We do this in three steps.

(a) i. Let $(p_i \otimes_Q q_j)$ and $(p_k \otimes_Q q_l)$ be any two arbitrary members of the set M, where

p_i, $p_k \varepsilon G_1$ and $q_j, q_l \varepsilon G_2$.

Using standard properties of Kronecker products (Appendix B),

$$(p_i \otimes_Q q_j).(p_k \otimes_Q q_l) = (p_i.p_k \otimes_Q q_j.q_l) \; ,$$

where the symbol . represents the operation of taking the conventional product of matrices. But $p_i \cdot p_k = p_p \varepsilon G_1$ for some $p \varepsilon Z_m$ and $q_j \cdot q_l = q_q \varepsilon G_2$ for some $q \varepsilon Z_n$.

$$(p_i \otimes_Q q_j)\cdot(p_k \otimes_Q q_l) = (p_p \otimes_Q q_q)\varepsilon M.$$

Thus, the set M is closed under multiplication.

ii. Now, let $(p_i \otimes_Q q_j)$, $(p_k \otimes_Q q_l)$ and $(p_p \otimes_Q q_q)$ $j,k,p\varepsilon Z_m$ and $j,l,q\varepsilon Z_n$ be three arbitrary members of **M.** Then using properties of Kronecker products, we may write

$$(p_i \otimes_Q q_j)\cdot((p_k \otimes_Q q_l)\cdot(p_p \otimes_Q q_q))$$

$$= (p_i\cdot(p_k\cdot\ p_p)) \otimes_Q (q_j\cdot(q_l\cdot\ q_q))\ .$$

Since $p_i, p_k, p_p \varepsilon G_1$ and $q_j, q_l, q_q \varepsilon G_2$, using the associativity properties of groups G_1 and G_2,

$$(p_i\cdot(p_k\cdot\ p_p)) \otimes_Q (q_j\cdot(q_l\cdot\ q_q))$$

$$= ((p_i\cdot\ p_k)\cdot p_p) \otimes_Q ((q_j\cdot\ q_l)\cdot q_q)\ .$$

Therefore,

$$(p_i \otimes_Q q_j)\cdot((p_k \otimes_Q q_l)\cdot(p_p \otimes_Q q_q))$$

$$= ((p_i\cdot\ p_k)\cdot p_p) \otimes_Q ((q_j\cdot\ q_l)\cdot q_q)$$

$$= ((p_i \otimes_Q q_j)\cdot(p_k \otimes_Q q_l))\cdot(p_p \otimes_Q q_q)\cdot$$

Members of the set M therefore have associative property under multiplication.

iii. If p_0 is the identity element of group G_1 and q_0 is the identity element of group G_2, $(p_0 \otimes_Q q_0)$ forms

the identity element in set M because for an arbitrary element $(p_i \otimes_Q q_j) \varepsilon M$; $i \varepsilon Z_m$, $j \varepsilon Z_n$, the following relation always holds:

$$(p_0 \otimes_Q q_0) \cdot (p_i \otimes_Q q_j) = (p_0 \cdot p_i \otimes_Q q_0 \cdot q_j) = (p_i \otimes_Q q_j).$$

iv. Let $(p_i \otimes_Q q_j) \varepsilon M$; $i \varepsilon Z_m$, $j \varepsilon Z_n$. Let p_0 and q_0 be the identity elements of the groups G_1 and G_2 respectively. Then there exist unique elements $p_k \varepsilon G_1$, $k \varepsilon Z_m$ and $q_l \varepsilon G_2$, $l \varepsilon Z_n$ such that

$$p_i \cdot p_k = p_k \cdot p_i = p_0 \text{ and } q_l \cdot q_j = q_0 \, .$$

Then $(p_k \otimes_Q q_l) \varepsilon M$, is the inverse element of $(p_i \otimes_Q q_j)$ because

$$(p_k \otimes_Q q_l) \cdot (p_i \otimes_Q q_j) = (p_k \cdot p_i \otimes_Q q_l \cdot q_j)$$

$$= (p_0 \otimes_Q q_0) = (p_i \otimes_Q q_j) \cdot (p_k \otimes_Q q_l) \, .$$

Thus, members of the set M form a multiplicative group G with conventional product of matrices forming the group operation. The identity element of this group is $(p_0 \otimes_Q q_0)$ where p_0 and q_0 are the identity elements of G_1 and G_2 respectively.

(b) We now note that G_1 and G_2 are abelian groups.

$$(p_i \otimes_Q q_j) \cdot (p_k \otimes_Q q_l) = (p_i \cdot p_k \otimes_Q q_j \cdot q_l)$$

$$= (p_k \cdot p_i \otimes_Q q_l \cdot q_j) = (p_k \otimes_Q q_l)(p_i \otimes_Q q_j)$$

for every p_i, $p_k \varepsilon G_1$; i, $k \varepsilon Z_m$ and every q_j, $q_l \varepsilon G_2$; j, $l \varepsilon Z_n$. Thus, group G is abelian.

(c) Since G_1 and G_2 are transitive abelian permutation groups, the ordering scheme described in Chapter 2 can be applied to their elements. Thus, p_i, $i \varepsilon Z_m$ is that member of G_1 which shifts the zeroth row of the 2-D signal X to the i-th row position when it premultiplies X. Hence, the matrix $p_i \varepsilon G_1$ is identified by the fact that the zeroth column of p_i has a 1 in the i-th place and zeros elsewhere. Similarly, q_j is that permutation matrix belonging to G_2, whose transpose, on postmultiplying X, shifts the zeroth column of X into the j-th column position. Thus, the matrix $q_j \varepsilon G_2$ has a 1 in the j-th position of its zeroth column.

Now, consider an arbitrary 1-D signal $x \varepsilon R^N$:

$$x = (x_0, x_1, \ldots, x_r, \ldots, x_{N-1})^T$$

We know that G is a transitive permutation group, if there exists for an arbitrarily specified integer $r \varepsilon Z_N$, a unique permutation matrix say $p_r \varepsilon G$, which by acting on x shifts the element x_0 into the r-th place. Since the index mapping f associated with the transformation Q is one-to-one, there is a unique ordered pair of integers (p,q) corresponding to $r \varepsilon Z_n$ such that

$$f^{-1}(r) = (p,q) \; ; \; r \varepsilon Z_N, \; p \varepsilon Z_m, \; q \varepsilon Z_n.$$

Then, from the way the matrix members of G are constructed and the ordering scheme employed for members of G_1 and G_2, it follows that the permutation matrix $P_r = (p_p \otimes_Q q_q)$ belonging to G is the element that shifts x_0 into the r-th position.

Thus, it is seen that G is transitive and is of degree and order N = m.n. In all we have thus established the following theorem:

Theorem 3.2.1: Let $Q:V \to R^N$ be a transformation which gives 1-D equivalents in R^N of 2-D signals in V. Then permuting the rows and columns of a 2-D signal $X \varepsilon V$ by permutation matrices p_i and q_j respectively, is in effect the same as permuting the equivalent 1-D signal of X viz., $x \varepsilon R^N$ by the permutation matrix $(p_i \otimes_Q q_j)$. If $p_i \varepsilon G_1$ and $q_j \varepsilon G_2$, for $i \varepsilon Z_m$ and $j \varepsilon Z_n$ where G_1 and G_2 are transitive abelian permutation groups of orders m and n respectively, then the set $M \stackrel{d}{=} \{p_i \otimes_Q q_j\}$ forms a transitive abelian group G of permutation matrices, which is of degree and order $N = m.n$.

We will now extend the ordering scheme mentioned earlier, to the members of G. To do this, recall the way we construct the Kronecker product matrix using the index mapping f associated with Q. Consider an element $P_{i,j} = (p_i \otimes_Q q_j) \varepsilon G$; $i \varepsilon Z_m$, $j \varepsilon Z_n$; $p_i \varepsilon G_1$ and $q_j \varepsilon G_2$. We note that

i. The zeroth column of $P_{i,j}$ is the Kronecker product of the zeroth columns of p_i and q_j respectively. (refer to remark 3.1.3).

ii. The zeroth column of $P_{i,j}$ has a 1 in the k-th position if f maps (i,j) onto k, and has zeros everywhere else. Also, because of the uniqueness of the mapping, there is no other member of G that has a 1 in the k-th position of its zeroth column.

iii. Thus, $P_{i,j}$ is that member of G which, on permuting a signal $x \varepsilon R^N$ shifts the zeroth element of x into the k-th position. We shall therefore denote it by P_k.

Remark 3.2.1: The element $(p_i \otimes_Q q_j) \varepsilon G$, $p_i \varepsilon G_1$, $i \varepsilon Z_m$; $q_j \varepsilon G_2$, $j \varepsilon Z_n$, is denoted by P_k if the mapping f associated with the transformation Q is such that it maps the pair of indices (i,j) onto $k \varepsilon Z_N$. With this notation, $P_k \varepsilon G$, $k \varepsilon Z_N$, is that member of G which shifts the zeroth entry of a signal $x = (x_0, x_1, \ldots, x_k, \ldots, x_{N-1})^T$ into the k-th position.

Having established that $G = p_i \otimes_Q q_j$, $p_i \varepsilon G_1$, $i \varepsilon Z_m$; $q_j \varepsilon G_2$, $j \varepsilon Z_n$, is a transitive abelian group of permutation matrices, and is of order $N = m.n$, we shall now show that G is indeed isomorphic to the direct product of G_1 and G_2.

For this purpose, let us define subsets H and K of G

$H \stackrel{d}{=} \{ p_i \otimes_Q q_0 \}$, where $p_i \varepsilon G_1$, $i \varepsilon Z_m$ and q_0 is the identity element of G_2 ; (3.2.5)

$K \stackrel{d}{=} \{ p_0 \otimes_Q q_j \}$, where $q_j \varepsilon G_2$, $j \varepsilon Z_n$ and p_0 is the identity element of G_1 . (3.2.6)

Using standard techniques in group theory [22,26] we find that H and K are subgroups of G. Now, since G is an abelian group, every subgroup of it must be a normal subgroup [26,p61] Therefore, H and K defined as in equations (3.2.5) and (3.2.6) are normal subgroups of G.

Then, we observe that

$(p_i \otimes_Q q_0) . (p_0 \otimes_Q q_j) = (p_i \otimes_Q q_j)$ for every $p_i \varepsilon G_1$ and every $q_j \varepsilon G_2$.

Hence, it follows that G is the internal direct product of its normal subgroups H and K, i.e.,

$$G = H.K. \tag{3.2.7}$$

Let us now define a function φ as follows:

$\varphi(p_i \otimes_Q q_0) = p_i$ for every $p_i \varepsilon G_1$.

Then φ is a homomorphism from H into G_1 because,

$\varphi((p_i \otimes_Q q_0).(p_k \otimes_Q q_0)) = \varphi((p_i.p_k \otimes_Q q_0))$

$= p_i.p_k = \varphi(p_i \otimes_Q q_0).\varphi(p_k \otimes_Q q_0)$ for every $p_i, p_k \varepsilon G_1$.

Further, from the definition of φ it is clear that it is one-to-one. Therefore, H is isomorphic to G_1. Similarly, it may be shown that K is isomorphic to G_2 i.e.,

$$H \doteq G_1, \tag{3.2.8}$$

and $$K \doteq G_2. \tag{3.2.9}$$

In equations (3.2.8) and (3.2.9) the symbol $\doteq$ is to be read as 'is isomorphic to'.

Equation (3.2.7) says that G is the internal direct product of its normal subgroups H and K defined as in equations (3.2.5) and (3.2.6) respectively. Thus, it follows [34 ,p.234] that G is isomorphic to the direct product of G_1 and G_2, i.e.,

$$G \doteq G_1 \times G_2. \tag{3.2.10}$$

We summarize this result as follows:

Remark 3.2.2: Given transitive abelian permutation groups G_1 of order m and G_2 of order n, the transitive abelian group G of degree and order $N = m.n$ formed by the set of permutation matrices $(p_i \otimes_Q q_j)$, $p_i \varepsilon G_1$, $i \varepsilon Z_m$; $q_j \varepsilon G_2$, $j \varepsilon Z_n$, is isomorphic to the direct product of G_1 and G_2.

Having thus obtained one-dimensional representations for two-dimensional signals and permutations, we are now ready to proceed to the final step - that of obtaining one-dimensional representation for two-dimensional permutation-invariant systems. This we do in the next section.

3.3 1-D P-I System Representation for 2-D P-I Systems

The various transformations involved in obtaining 1-D representations of 2-D systems are shown diagrammatically in Fig. 3.2.

$$\begin{tikzcd} V \arrow[r, "Q"] \arrow[d, "T"'] & R^N \arrow[d, "t"] \\ V \arrow[r, "Q"'] & R^N \end{tikzcd}$$

Fig. 3.2: 1-D Equivalent of 2-D P-I Systems

In this figure,

V is the 2-D signal space of all real $m \times n$ matrices,

R^N is the usual vector space of N-tuples of reals, and

Q is a linear transformation from V to R^N (refer section 3.1).

Further, T is any finite discrete linear system on V and t is its 1-D equivalent representation under the transformation Q.

The system t is in general given by

$$t = Q\,TQ^{-1} \tag{3.3.1}$$

Suppose the 2-D signals X, $Y \varepsilon V$ are respectively the input and output signals for the system T and that x, $y \varepsilon R^N$ are the 1-D equivalent signals of respectively X and Y. Then we have,

$$x = Q(X)$$

$$y = Q(TX) = Q(Y) = tx = tQ(X). \tag{3.3.2}$$

If we now suppose that T is a 2-D P-I system belonging to a certain class, we would like to examine whether its 1-D equivalent representation defined through equation (3.3.1) is also permutation-invariant, and if it is, then we would like to determine the class to which it belongs. To be specific, let T be a 2-D P-I system relative to G_1 of order m and G_2 of order n.

Consider the 2-D signal $X_p \varepsilon V$ obtained from $X \varepsilon V$ as

$$X_p = p_k\, X\, q_1^T \ ,\ p_k \varepsilon G_1,\ q_1 \varepsilon G_2 \ ;\ k \varepsilon Z_m,\ l \varepsilon Z_n.$$

X_p is thus obtained from X by permuting its rows by the matrix $p_k \varepsilon G_1$ and the columns by the matrix $q_1 \varepsilon G_2$. Let X_p be now given as input to T. Since T is a 2-D permutation-invariant system, using equation (2.2.4), and subsequently equation (3.2.4),

$$TX_p = T(p_k\, X\, q_1^T) = p_k(TX)q_1^T$$

$$Q(TX_p) = Q(p_k(TX)q_1^T) = (p_k \otimes_Q q_1)Q(TX). \qquad (3.3.3)$$

In view of remark 3.2.1 and equation (3.3.2) we may now rewrite the above equation as

$$Q(TX_p) = P_p(Q(TX)) = P_p\ tx\ , \qquad (3.3.4)$$

where P_p is a permutation matrix belonging to the transitive abelian group of permutation matrices G which is defined by

$$G \stackrel{d}{=} \{p_k \otimes_Q q_1\} \ ,\ p_k \varepsilon G_1,\ q_1 \varepsilon G_2.$$

Again,

$$tQX_p = t(p_k \otimes_Q q_1)Q(X) = tP_p x\ . \qquad (3.3.5)$$

Then from equation (3.3.1),

$$Q(TX_p) = tQX_p\ . \qquad (3.3.6)$$

From equations (3.3.4), (3.3.5) and (3.3.6), we then have,

$$P_p\, t\, x = t\, P_p\, x\,. \tag{3.3.7}$$

Since p_k and q_1 are arbitrarily chosen members of G_1 and G_2 respectively, equation (3.3.7) is true for any arbitrary member of G.

Thus, equation (3.3.7) implies that t is a permutation-invariant system relative to G, a transitive abelian group of permutation matrices which is isomorphic to the direct product $G_1 \times G_2$ and defined by

$$G = \{ p_k \otimes_Q q_1 \}\,,\; p_k \varepsilon G_1,\; k \varepsilon Z_m \;;\; q_1 \varepsilon G_2,\; 1 \varepsilon Z_n.$$

Thus, the following theorem is fully established:

Theorem 3.3.1: If T is a 2-D permutation-invariant system on V relative to groups G_1 of order m and G_2 of order n, then t; the 1-D equivalent of T is also permutation-invariant; the permutation-invariance of t is relative to a transitive abelian permutation group G of order $N = m.n$ formed by the set of permutation matrices $\{ p_i \otimes_Q q_j \}$, $p_i \varepsilon G_1$, $i \varepsilon Z_m$; $q_j \varepsilon G_2$, $j \varepsilon Z_n$.

Remark 3.3.1: If T is a 2-D P-I system, in view of theorem 3.3.1, t, the 1-D equivalent of T under the transformation Q will be referred to as the equivalent 1-D P-I system of T under Q.

Having thus established the equivalence between 2-D and 1-D P-I systems, our next endeavour is to obtain explicit expressions through which, given any 2-D P-I system T, its equivalent 1-D P-I system t can be fully determined under the assumed linear transformation Q from V to R^N.

Let S be a class of 2-D P-I systems on V, the space of real m x n matrices, relative to G_1 and G_2 of orders m and n respectively. Then a system $T \varepsilon S$ is expressible as (Chapter 2, p 33).

$$T = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} B_{i,j} ,$$

where, $s_{i,j}$ are the entries of s, the unit response matrix of T and $B_{i,j}$ are the basic 2-D P-I system of S. Therefore, for any arbitrary signal $X \varepsilon V$, we have,

$$TX = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} B_{i,j} \right) X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} (p_i X q_j^T) .$$

Now let Q be a transformation which gives 1-D equivalents of 2-D signals. Let t denote the 1-D equivalent of T under Q. Then referring to equation (3.3.1),

$$T = Q^{-1} t Q ,$$

$$TX = Q^{-1} t Q X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} (p_i X q_j^T) .$$

But $QX = x$, the 1-D equivalent of X, under the transformation Q.

Therefore,

$$tx = Q\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j}(p_i\ X\ q_j^T)\right) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} Q(p_i X\ q_j^T).$$

But $\quad Q(p_i\ X\ q_j^T) = (p_i \otimes_Q q_j)QX = (p_i \otimes_Q q_j)x.$

Finally, using (3.2.4)

$$tx = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j}(p_i \otimes_Q q_j)x \quad \text{for every } x \varepsilon R^N,$$

i.e., $\quad t = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j}(p_i \otimes_Q q_j)\ ;\ p_i \varepsilon G_1,\ i \varepsilon Z_m;\ q_j \varepsilon G_2, j \varepsilon Z_n.$

(3.3.8)

Thus, we have

Theorem 3.3.2: Let T be a 2-D P-I system belonging to a class S relative to groups G_1 and G_2 of orders m and n respectively. Then t, the 1-D equivalent of T under Q is given by

$$t = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j}(p_i \otimes_Q q_j)\ ;\ p_i \varepsilon G_1,\ i \varepsilon Z_m\ ;$$
$$q_j \varepsilon G_2,\ j \varepsilon Z_n,$$

where the $s_{i,j}$'s are the entries of s, the unit response matrix of T. Further, t is a 1-D P-I system relative to the Group G (Theorem 3.2.1).

It would be more convenient if we put equation (3.3.8) in the conventional form, i.e., one wherein the system matrix of t is expressed in terms of the entries of its own unit sample response vector. For this, however, we have to first establish a relationship between the N entries of the m x n unit response matrix $s = T_{0,0}$ of the 2-D P-I system T on the one hand, and the N entries of the unit sample vector $S^{(0)}$ of the equivalent 1-D P-I system t on the other. The unit sample signal for the 2-D P-I systems on V has been taken (remark 2.1.1) to be $\Delta_{0,0}$, an m x n matrix with a 1 in the (0,0)-th position and zeros everywhere else; while the unit sample signal for the 1-D P-I system on R^N is e_0, the N-length column vector with a 1 in its zeroth place and zeros elsewhere

$$\Delta_{0,0} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix},$$

and $$e_0 = (1\ 0 \cdots 0)^T.$$

Now, we recall (remark 3.1.3) that the transformation Q from V onto R^N is so chosen that the (0,0)-th element of any 2-D signal $X \epsilon V$ is always mapped onto the 0-th entry of the 1-D equivalent of X. Thus,

$$e_0 = Q\,\Delta_{0,0}\,.$$

Then from Fig. 3.3.1 it follows that

$$s^{(0)} \stackrel{d}{=} t\,e_0 = Q(T\,\Delta_{0,0}) = Q(T_{0,0}) \stackrel{d}{=} Q(s),$$

i.e., $s^{(0)} = Q(s)$, (3.3.9)

where $s^{(0)}$ is the unit sample response of the equivalent 1-D P-I system t and s is the unit response matrix of the 2-D P-I system T. Thus, in view of equation (3.3.9) and remark 3.2.1, we may now rewrite equation (3.3.8) as

$$t = \sum_{k=0}^{N-1} s_k\,P_k \qquad ; \qquad P_k \varepsilon G\,, \tag{3.3.10}$$

where s_k, $k\varepsilon Z_N$ is the k-th entry of the unit sample response vector $s^{(0)}$ of the 1-D P-I system t, and P_k is the k-th member of the transitive abelian group of permutation matrices G relative to which t is defined. Further, if f the index mapping associated with Q gives

$$k = f(i,j) \qquad ; \qquad i\varepsilon Z_m,\ j\varepsilon Z_n,\ k\varepsilon Z_N\,,$$

then $s_k = s_{i,j}\,,$

and $P_k = p_i \otimes_Q q_j\,.$ (3.3.11)

From the foregoing, it is clear that different linear transformations Q from V to R^N lead to different equivalent

1-D systems for the same 2-D system T. The following examples illustrate this point and also help to consolidate our ideas regarding equivalent 1-D P-I systems for 2-D P-I systems:

Example 3.3.1: Let V be the space of real 2 x 3 matrices so that m = 2 and n = 3. Let $\Delta_{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$, the basis elements of V, be ordered lexicographically, i.e., the index mapping f associated with the transformation Q be

$$k = f(i,j) = ni + j = 3i + j, \; i \varepsilon Z_m, \; j \varepsilon Z_n.$$

Let G_1 and G_2 be transitive abelian cyclic groups of permutation matrices given by

$$G_1 = \{ p_0, p_1 \}, \text{ where, } p_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } p_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix};$$

and $$G_2 = \{ q_0, q_1, q_2 \}, \text{ where, } q_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$q_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, q_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

If T, a 2-D P-I system relative to G_1 and G_2 has a unit response matrix s given by

$$s = \begin{bmatrix} 3 & 1 & 0 \\ 2 & 4 & 2.5 \end{bmatrix},$$

then for any arbitrary signal X

$$X = \begin{bmatrix} X_{0,0} & X_{0,1} & X_{0,2} \\ X_{1,0} & X_{1,1} & X_{1,2} \end{bmatrix}$$

the 2-D P-I system T is interms of the basic systems,

$$TX = 3B_{0,0}\,X + 1.B_{0,1}\,X + 0.B_{0,2}\,X + 2.B_{1,0}\,X$$
$$+ 2.5B_{1,2}\,X.$$

The basic systems $B_{i,j}$ are given by

$$B_{i,j}\,X = p_i\,X\,q_j^T\ ;\ p_i \varepsilon G_1,\ i\varepsilon Z_2 \text{ and } q_j \varepsilon G_2,\ j\varepsilon Z_3.$$

In detail,

$$TX = 3\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}[X]\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix} + 1\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}[X]\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}^T$$

$$+ 2\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}[X]\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}^T + 4\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}[X]\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}^T$$

$$+ 2.5\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}[X]\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}^T$$

$$= \begin{bmatrix} (3X_{0,0}+X_{0,2}+2X_{1,0}+2.5X_{1,1}+4X_{1,2}) & (X_{0,0}+3X_{0,1}+4X_{1,0}+2X_{1,1}+2.5X_{1,2}) & (X_{0,1}+3X_{0,2}+2.5X_{1,0}+4X_{1,1}+2X_{1,2}) \\ (2X_{0,0}+2.5X_{0,1}+4X_{0,2}+3X_{1,0}+X_{1,2}) & (4X_{0,0}+2X_{0,1}+2.5X_{0,2}+X_{1,0}+3X_{1,1}) & (2.5X_{0,0}+4X_{0,1}+2X_{0,2}+X_{1,1}+3X_{1,2}) \end{bmatrix}$$

and $$Q(TX) = \begin{bmatrix} (3X_{0,0} + X_{0,2} + 2X_{1,0} + 2.5X_{1,1} + 4X_{1,2}) \\ (X_{0,0} + 3X_{0,1} + 4X_{1,0} + 2X_{1,1} + 2.5X_{1,2}) \\ (X_{0,1} + 3X_{0,2} + 2.5X_{1,0} + 4X_{1,1} + 2X_{1,2}) \\ (2X_{0,0} + 2.5X_{0,1} + 4X_{0,2} + 3X_{1,0} + X_{1,2}) \\ (4X_{0,0} + 2X_{0,1} + 2.5X_{0,2} + X_{1,0} + 3X_{1,1}) \\ (2.5X_{0,0} + 4X_{0,1} + 2X_{0,2} + X_{1,1} + 3X_{1,2}) \end{bmatrix}$$

The equivalent 1-D P-I system under the assumed transformation Q, represented by the system matrix t is given by

$$t = 3 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes_Q \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$+ 2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 4 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$+ 2.5 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$= 3 \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} + 1 \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} + 2 \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$+ 4 \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} + 2.5 \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 0 & 1 & 2 & 2.5 & 4 \\ 1 & 3 & 0 & 4 & 2 & 2.5 \\ 0 & 1 & 3 & 2.5 & 4 & 2 \\ 2 & 2.5 & 4 & 3 & 0 & 1 \\ 4 & 2 & 2.5 & 1 & 3 & 0 \\ 2.5 & 4 & 2 & 0 & 1 & 3 \end{bmatrix}.$$

$$QX = (X_{0,0}\ X_{0,1}\ X_{0,2}\ X_{1,0}\ X_{1,1}\ X_{1,2})^T.$$

It may be verified that $t(QX) = Q(TX)$.

Note that the unit sample response of the equivalent 1-D P-I system t, represented by the zeroth column of the system matrix t, is obtained by reading off the entries of the unit response matrix s of the 2-D P-I system, in a lexicographic manner, since in this example the index mapping f associated with Q is the lexicographic way of ordering of pairs of indices.

Example 3.3.2: Assuming the same 2-D P-I system as in the previous example, let us now use a transformation Q that orders the basis elements $\Delta_{i,j}$, $i\varepsilon Z_2$, $j\varepsilon Z_3$, of V in accordance with the index mapping given in example 3.2.2, viz.,

$$k = f(i,j) = (3i + 4j) \bmod 6,\ i\varepsilon Z_2,\ j\varepsilon Z_3,\ k\varepsilon Z_6.$$

Then, $TX =$

$$\begin{bmatrix} (3X_{0,0}+X_{0,2}+2X_{1,0}+2.5X_{1,1}+4X_{1,2}) & (X_{0,0}+3X_{0,1}+4X_{1,0}+2X_{1,1}+2.5X_{1} \ldots \\ (2X_{0,0}+2.5X_{0,1}+4X_{0,2}+3X_{1,0}+X_{1,2}) & (4X_{0,0}+2X_{0,1}+2.5X_{0,2}+X_{1,0}+3X_{1} \ldots \end{bmatrix}$$

$$(X_{0,1}+3X_{0,2}+2.5X_{1,0}+4X_{1,1}+2X_{1} \ldots$$

$$(2.5X_{0,0}+4X_{0,1}+2X_{0,2}+X_{1,1}+3X_{1,} \ldots$$

But $Q(TX)$ is now given by

$$Q(TX) = \begin{bmatrix} (3X_{0,0} + X_{0,2} + 2X_{1,0} + 2.5X_{1,1} + 4X_{1,2}) \\ (4X_{0,0} + 2X_{0,1} + 2.5X_{0,2} + X_{1,0} + 3X_{1,1}) \\ (X_{0,1} + 3X_{0,2} + 2.5X_{1,0} + 4X_{1,1} + 2X_{1,2}) \\ (2X_{0,0} + 2.5X_{0,1} + 4X_{0,2} + 3X_{1,0} + X_{1,2}) \\ (X_{0,0} + 3X_{0,1} + 4X_{1,0} + 2X_{1,1} + 2.5X_{1,2}) \\ (2.5X_{0,0} + 4X_{0,1} + 2X_{0,2} + X_{1,1} + 3X_{1,2}) \end{bmatrix}$$

$$t = 3 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes_Q \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$+ 2 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 4 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$+ 2.5 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes_Q \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$= 3\begin{bmatrix} 1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1 \end{bmatrix} + 1\begin{bmatrix} 0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0 \end{bmatrix} + 2\begin{bmatrix} 0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0 \end{bmatrix}$$

$$+ 4\begin{bmatrix} 0&0&0&0&0&1\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0 \end{bmatrix} + 2.5\begin{bmatrix} 0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\\1&0&0&0&0&0 \end{bmatrix}$$

$$= \begin{bmatrix} 3&2.5&1&2&0&4\\4&3&2.5&1&2&0\\0&4&3&2.5&1&2\\2&0&4&3&2.5&1\\1&2&0&4&3&2.5\\2.5&1&2&0&4&3 \end{bmatrix}.$$

From the given index mapping,

$$QX = (X_{0,0}\ X_{1,1}\ X_{0,2}\ X_{1,0}\ X_{0,1}\ X_{1,2})^T$$

So that

$$tQX = \begin{bmatrix} (3X_{0,0} + 2.5X_{1,1} + X_{0,2} + 2X_{1,0} + 4X_{1,2}) \\ (4X_{0,0} + 3X_{1,1} + 2.5X_{0,2} + 1X_{1,0} + 2X_{0,1}) \\ (4X_{1,1} + 3X_{0,2} + 2.5X_{1,0} + 1X_{0,1} + X_{1,2}) \\ (2X_{0,0} + 4X_{0,2} + 3X_{1,0} + 2.5X_{0,1} + 1X_{1,2}) \\ (1X_{0,0} + 2X_{1,1} + 4X_{1,0} + 3X_{0,1} + 2.5X_{1,2}) \\ (2.5X_{0,0} + 1X_{1,1} + 2X_{0,2} + 4X_{0,1} + 3X_{1,2}) \end{bmatrix} = Q(TX)$$

Observe the difference in the form of the system matrices of the equivalent 1-D P-I systems obtained in the two cases, under the different transformations used. The question then naturally arises: 'Are there some preferred transformations which, for a given problem on hand, lead to a more desirable form of an equivalent 1-D P-I system for a given 2-D P-I system'? This question has been investigated in depth in Chapter 6 in connection with 1-D implementation of 2-D filtering in the Fourier and Walsh domains.

It must be pointed out that given the equivalent 1-D P-I system obtained under a specific known transformation Q, we can always reconstruct the original 2-D P-I system without any ambiguity. To be specific, let t be the equivalent 1-D P-I system defined relative to G, obtained under a known transformation Q from V to R^N. Then,

$$t = \sum_{k=0}^{N-1} s_k P_k ,$$

where s_k, $k \varepsilon Z_N$ are the entries in the unit sample response vector $S^{(0)}$ and P_k, $k \varepsilon Z_N$ belong to G.

Now, since the index mapping f associated with Q is one-to-one, any specific integer k belonging to Z_N is mapped onto a unique ordered pair of integers (i,j), $i \varepsilon Z_m$, $j \varepsilon Z_n$ by the inverse mapping f^{-1}. Therefore,

$$t = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} P_{i,j} . \qquad (3.3.12)$$

But $P_{i,j} \overset{d}{=} p_i \otimes_Q q_j$ (remark 3.2.1) and $t = QTQ^{-1}$ so that for any $x \varepsilon R^N$,

$$tx = QTQ^{-1}x = QTX,$$

where X is the unique 2-D representation of x under the inverse transformation Q^{-1}. Therefore, equation (3.3.12) may be written as

$$QTX = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (s_{i,j}(p_i \otimes_Q q_j)x),$$

i.e., $$TX = Q^{-1}\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j}(p_i \otimes_Q q_j)x\right)$$

$$= \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \; Q^{-1}(p_i \otimes_Q q_j)(QX)\right).$$

Now, using equation (3.2.4),

$$TX = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \; p_i \; X \; q_j^T = \left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \; B_{i,j}\right)X,$$

for every $X \varepsilon V$,

where $B_{i,j}$ is given by (refer equation 2.5.1)

$$B_{i,j}X = p_i \; X \; q_j^T \;, \quad \text{for every } X \varepsilon V,$$

i.e. $$T = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \; B_{i,j} \; . \tag{3.3.13}$$

Thus, since the $s_{i,j}$'s and $B_{i,j}$'s, $i\varepsilon Z_m$, $j\varepsilon Z_n$, are determined uniquely from the respective s_k's and P_k's, $k\varepsilon Z_N$ of the given 1-D P-I system t, the 2-D P-I system T is uniquely determined from equation (3.3.13).

3.3.1 Eigenvalues and Eigenvectors of the Equivalent 1-D P-I System

Let T be a 2-D P-I system on V and let T belong to a class S defined relative to G_1 and G_2. If t be the 1-D P-I system that is equivalent to T under the transformation Q from V to R^N, then we have, (refer equation (2.6.8))

$$Q(Th_N^{i,j}) = \left(\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\, \sigma_m^{i,k}\, \sigma_n^{j,l}\right) Q(h_N^{i,j}) \,. \quad (3.3.14)$$

But, $Q(Th_N^{i,j}) = t(Q(h_N^{i,j})) = t(Q((h_m^i)(h_n^j)^T)) = t(h_m^i \otimes_Q h_n^j)$.

Using equation (2.6.9), equation (3.3.14) may be rewritten as

$$t(h_m^i \otimes_Q h_n^j) = \left(\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} s_{k,l}\, \sigma_m^{i,k}\, \sigma_n^{j,l}\right)(h_m^i \otimes_Q h_n^j)$$

$$= \sigma_T^{i,j}\, Q(h_N^{i,j}) \,.$$

Thus, if $h_N^{i,j} = (h_m^i).(h_n^j)^T$, is the i,j-th eigenvector of the 2-D P-I system T, the corresponding eigenvector of t, the equivalent 1-D P-I system of T under the transformation Q from V onto R^N, is given by $Q(h_N^{i,j}) = h_m^i \otimes_Q h_n^j$; and the set

$h_m^i \otimes_Q h_n^j$, $i \varepsilon Z_m$, $j \varepsilon Z_n$ form the common set of eigenvectors of the equivalent class of 1-D P-I systems obtained from the class S of 2-D P-I systems under the transformation Q.

Also, if the index mapping f associated with Q be

$$f : (i,j) \to p \qquad ; \qquad i \varepsilon Z_m,\ j \varepsilon Z_n \text{ and } p \varepsilon Z_N .$$

Then, the p-th eigenvector of t, viz., H_N^p, is given by

$$H_N^p = Q(h_N^{i,j}) \qquad ; \qquad p \varepsilon Z_N,\ i \varepsilon Z_m,\ j \varepsilon Z_n , \tag{3.3.15}$$

where $h_N^{i,j}$ is the (i,j)-th eigenvector of the 2-D P-I system T. Further, if $\sigma_T^{i,j}$ is the eigenvalue with which the eigenvector $h_N^{i,j}$ of T is associated, then the eigenvector H_N^p of t is associated with the eigenvalue $\sigma_t^p = \sigma_T^{i,j}$.

Thus, we have arrived at explicit expressions for the eigenvalues and eigenvectors of the equivalent 1-D P-I system t in terms of the eigenvalues and eigenvectors of T, the 2-D P-I system from which t is obtained under a transformation Q.

We would like to point out that the properties of 2-D P-I systems discussed in Chapter 2 as well as the equivalence between the 2-D P-I systems and 1-D P-I systems discussed in the present chapter, could have been obtained by adopting a different approach, wherein we regard V, the vector space of all real m x n matrices, and equivalently, R^N, the vector space of all real N-tuples, as tensor product spaces.

CHAPTER 4

TRANSFORM DOMAIN CHARACTERIZATION OF 2-D P-I SYSTEMS

In this chapter, first a generalized 2-D finite discrete transform of 2-D P-I systems is given and it is shown that the 2-D DFT and 2-D DWT are special cases of this 2-D finite discrete transform (2-D FDT). This is followed by a transform domain description of 2-D P-I systems wherein it is shown that the 2-D FDT satisfies a generalized convolutional theorem. The notion of transfer function of a 2-D P-I system is next introduced and finally, the relationship between the transfer characteristics of a 2-D P-I system and its equivalent 1-D P-I system is discussed.

4.1 Generalized 2-D Finite Discrete Transform

In section 2.6 it was shown that members of a class of 2-D P-I systems have a common set of linearly independent orthonormal eigenvectors which span the pertinent signal

space of that class. Utilizing this result, we derive in the present section a generalized 2-D finite discrete transform (2-D FDT) of 2-D P-I systems.

Let T be a 2-D P-I system relative to G_1 and G_2 of orders m and n respectively and let $N = m.n$. Then, as shown in section 2.6, the set of eigenvectors of T, viz., $h_N^{i,j}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$ forms a basis for the space W of complex m x n matrices (refer to remark 2.6.1). Thus, any arbitrary 2-D signal $x \varepsilon W$ may be written as

$$x = \frac{1}{m.n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j} \, h_N^{i,j} = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j} h_m^i (h_n^j)^T. \tag{4.1.1}$$

In equation 4.1.1 we have made use of the fact that $h_N^{i,j}$, the (i,j)-th eigenvector of T is equal to $(h_m^i).(h_n^j)^T$ where h_m^i is the i-th eigenvector of the class of 1-D P-I systems relative to G_1 and h_n^j is the j-th eigenvector of the class of 1-D P-I systems relative to G_2. Now recalling that (see Appendix A) h_m^i is the i-th column of the generalized Hadamard matrix H_m of order m [35] equation (4.1.1) may be put in matrix form as

$$x = \frac{1}{N} (H_m \, X \, H_n^T). \tag{4.1.2}$$

Therefore,

$$X = N(H_m^{-1} \, x \, (H_n^T)^{-1}).$$

But $H_m^{-1} = \frac{1}{m} H_m^*$,

where H_m^* is the complex conjugate transpose of H_m.

Therefore,

$$X = H_m^* \; x \; H_n^{*\,T}.$$

The above equation may be rewritten as

$$X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^i \, x_{i,j} \, (\bar{h}_n^j)^T = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} \, \bar{h}_N^{i,j},$$

where $\bar{h}_N^{i,j}$ is the complex conjugate of $h_N^{i,j}$, the (i,j)-th eigenvector of T. Thus,

$$X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} \, \bar{h}_N^{i,j} \quad , \qquad (4.1.3)$$

and $$x = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j} \, h_N^{i,j} \; . \qquad (4.1.4)$$

Using the relation $h_N^{i,j} = (h_m^i).(h_n^j)^T$ we may rewrite equations (4.1.3) and (4.1.4) alternatively as

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} \; x_{i,j} \; \bar{h}_n^{l,j} \; ; \; k\varepsilon Z_m, \; l\varepsilon Z_n, \qquad (4.1.5)$$

and $$x_{i,j} = \frac{1}{N} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} h_m^{k,i} \, X_{k,l} \, h_n^{l,j} \; ; \; i\varepsilon Z_m, \; j\varepsilon Z_n. \qquad (4.1.6)$$

Definition 4.1.1: The pair of equations (4.1.3) and (4.1.4) or alternatively, equations (4.1.5) and (4.1.6) will be called the generalized 2-D finite discrete transform (2-D FDT) pair. X will be referred to as the 2-D FDT of x, and x the inverse 2-D FDT of X.

Just as the matrices associated with the discrete Fourier transform (DFT) and the discrete Walsh transform (DWT) are special cases of the generalized Hadamard matrix [35], it can be shown that the familiar 2-D DFT and 2-D DWT are themselves special cases of the 2-D FDT enunciated above. We will now examine this question in detail.

4.1.1 2-D Discrete Fourier Transform (2-D DFT)

Suppose the system T considered in the previous section is a 2-D cyclic P-I system, i.e., a 2-D P-I system relative to G_1 and G_2 which are cyclic permutation groups of orders m and n respectively. Since the number of invariants for a cyclic group is only one, r = 1 for G_1 as well as G_2. Further, $h_m^{k,i}$, the k-th entry of the i-th eigenvector of a class of 1-D P-I systems relative to G_1 of order m and $h_n^{l,j}$, the l-th entry of the j-th eigenvector of a class of 1-D P-I systems relative to G_2 of order n, will be given by (refer to equations A.24 and A.25 of Appendix A)

$$\bar{h}_m^{k,i} = \gamma_m^{-ki} \quad , \text{ and}$$

$$\bar{h}_n^{l,j} = \gamma_n^{-lj},$$

where $\gamma_p = \exp(\sqrt{-1}\,\frac{2\pi}{p})$.

Thus, equations (4.1.5) and (4.1.6) take the form

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \gamma_m^{-ki}\, x_{i,j}\, \gamma_n^{-lj} \; ; \; k\varepsilon Z_m, l\varepsilon Z_n \, , \tag{4.1.7}$$

and

$$x_{i,j} = \frac{1}{N} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} \gamma_m^{ki}\, X_{k,l}\, \gamma_n^{lj} \; ; \; i\varepsilon Z_m, j\varepsilon Z_n \, . \tag{4.1.8}$$

Equations (4.1.7) and (4.1.8) may be recognized as the defining equations of the 2-D DFT pair [40].

4.1.2 2-D Discrete Walsh-Hadamard Transform (2-D DWT)

Now, suppose that T is a 2-D dyadic P-I system relative to the pair of dyadic groups G_1 of order $m = 2^{r_1}$ and G_2 of order $n = 2^{r_2}$. Then (refer to equations A.24 and A.25 of Appendix A)

$$\bar{h}_m^{k,j} = \prod_{\alpha=0}^{r_1-1} \gamma_\alpha^{-k_\alpha i_\alpha} \quad ; \; k,\ i\varepsilon Z_m \, , \tag{4.1.9}$$

and $$\bar{h}_n^{l,j} = \prod_{\alpha=0}^{r_2-1} \gamma_\alpha^{-l_\alpha j_\alpha} \quad ; \; l,\ j\varepsilon Z_n \, , \tag{4.1.10}$$

where $\gamma_\alpha = \exp(\sqrt{-1}\,\frac{2\pi}{2}) = -1$,

and k_α, i_α, l_α and j_α are now digits in the binary expansion of the integers k,i,l and j respectively so that they are either 0 or 1. Therefore, we may write

$$h_m^{k,i} = \prod_{\alpha=0}^{r_1-1} (-1)^{k_\alpha i_\alpha} = (-1)^{\sum_{\alpha=0}^{r_1-1} k_\alpha i_\alpha} \quad ; \; k,i \varepsilon Z_m , \tag{4.1.11}$$

and

$$h_n^{l,j} = \prod_{\alpha=0}^{r_2-1} (-1)^{l_\alpha j_\alpha} = (-1)^{\sum_{\alpha=0}^{r_2-1} l_\alpha j_\alpha} \quad ; \; l,j \varepsilon Z_n . \tag{4.1.12}$$

$h_m^{k,i}$ and $h_n^{l,j}$ as given by equations (4.1.11) and (4.1.12) are recognized to specify discrete Walsh functions in what is called Hadamard order or natural order [36]. Substituting for $h_m^{k,i}$ and $h_n^{l,j}$ in equations (4.1.5) and (4.1.6) of the 2-D FDT pair gives

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} (-1)^{\sum_{\alpha=0}^{r_1-1} k_\alpha i_\alpha + \sum_{\alpha=0}^{r_2-1} l_\alpha j_\alpha} , \tag{4.1.13}$$

and

$$x_{i,j} = \frac{1}{N} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} X_{k,l} (-1)^{\sum_{\alpha=0}^{r_1-1} k_\alpha i_\alpha + \sum_{\alpha=0}^{r_2-1} l_\alpha j_\alpha} . \tag{4.1.14}$$

Equations (4.1.13) and (4.1.14) are now recognized [37] as the 2-D Walsh-Hadamard transform (2-D DWT) pair with the transform in the natural or Hadamard order. A sequency ordered form of 2-D DWT can be obtained by writing $h_m^{k,i}$ and $h_n^{l,j}$ in the modified form given below.

$$h_m^{k,i} = \prod_{\alpha=0}^{r_1-1} (-1)^{k_\alpha(i_{r_1-\alpha}+ i_{r_1-\alpha-1})}$$

$$= (-1)^{\sum_{\alpha=0}^{r_1-1} k_\alpha(i_{r_1-\alpha}+ i_{r_1-\alpha-1})} \quad ; \; k,\ i\varepsilon Z_m \, ;$$

and $$h_n^{l,j} = \prod_{\alpha=0}^{r_2-1} (-1)^{l_\alpha(j_{r_2-\alpha}+ j_{r_2-\alpha-1})}$$

$$= (-1)^{\sum_{\alpha=0}^{r_2-1} l_\alpha(j_{r_2-\alpha}+ j_{r_2-\alpha-1})} \quad ; \; l,\ j\varepsilon Z_n \, .$$

In this form, $h_m^{k,i}$ and $h_n^{l,j}$ specify discrete Walsh functions in the sequency order and when they are in this form, we shall denote them by $w_m^{k,i}$ and $w_n^{l,j}$ respectively.

Correspondingly, the 2-D FDT now takes the form

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} w_m^{k,i} \; x_{i,j} \; w_n^{l,j} \, , \tag{4.1.15}$$

and $$x_{i,j} = \frac{1}{N} \sum_{k=0}^{m-1} \sum_{l=0}^{n-1} w_m^{k,i} X_{k,l} w_n^{l,j} . \tag{4.1.16}$$

When written in the matrix form, this sequency ordered 2-D DWT pair becomes

$$X = W_m x W_n , \tag{4.1.17}$$

and $$x = \frac{1}{N} (W_m X W_n), \tag{4.1.18}$$

where, W_m and W_n are sequency ordered Hadamard matrices of orders m and n respectively. The pair of equations (4.1.17) and (4.1.18) is called the sequency ordered 2-D DWT pair [36].

Having shown that the 2-D DFT and 2-D DWT follow as special cases of the 2-D FDT, we will now examine some basic properties of this generalized transform.

4.1.3 Basic Properties of the 2-D FDT

(1) Linearity: According to this property, if $T(x)$ denotes the 2-D FDT of a signal $x \varepsilon W$ then

$$T(\alpha_1 x + \alpha_2 y) = \alpha_1 T(x) + \alpha_2 T(y) \quad ; \text{ for every } x,y \varepsilon W \; ; \; \alpha_1, \alpha_2 \varepsilon C ,$$

where W is the vector space of m x n matrices with entries from C. This property follows directly from the way the transform itself has been defined.

(2) Normalization property: $(T(\Delta_{0,0}))_{k,l}$, the (k,l)-th element of the 2-D FDT of the 2-D unit sample signal $\Delta_{0,0}$, equals 1 for every k belonging to Z_m and every l belonging to Z_n,

i.e., $(T(\Delta_{0,0}))_{k,l} = 1$ for every $k \varepsilon Z_m$, every $l \varepsilon Z_n$.

To verify this, put $x = \Delta_{0,0}$ in the equation (4.1.5). Since $x_{0,0} = 1$ and all other elements of x are zero, it follows that

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i}\ x_{i,j}\ \bar{h}_n^{l,j} = \bar{h}_m^{k,0}\ .1.\ \bar{h}_n^{l,0}.$$

$\bar{h}_m^{k,0}$ for $k = 0,1,2, - - - , (m-1)$ represents entries in the zeroth column of H_m^*. Similarly, $\bar{h}_n^{l,0}$ for $l = 0,1,2, - - - , (n-1)$ represents elements in the zeroth column of H_n^*. But all the entries in the zeroth columns of H_m^* and H_n^* are equal to 1. Therefore,

$$X_{k,l} = 1 \quad \text{for every } k \varepsilon Z_m \text{ and every } l \varepsilon Z_n,$$

i.e., $(T(\Delta_{0,0}))_{k,l} = 1$ for every $k \varepsilon Z_m$ and every $l \varepsilon Z_n$.

(3) Permutation Property: This property relates the 2-D FDT of any 2-D signal x with that of a permuted 2-D signal $\underline{x}$ obtained by permuting the rows and columns of x by members

of transitive abelian permutation groups G_1 and G_2 of appropriate orders. To be specific, it says that if $\underline{X}$ is the 2-D FDT of $\underline{x}$ and X, the 2-D FDT of x, where $\underline{x} = p_p \times q_q^T$; $p_p \varepsilon G_1$, $q_q \varepsilon G_2$, $p \varepsilon Z_m$, $q \varepsilon Z_n$, then

$$\underline{X}_{k,l} = \bar{h}_m^{k,p} \; \bar{h}_n^{l,q} \; X_{k,l} .$$

Proof: Since $\underline{x} = p_p \times q_q^T$, from equation (2.3.5) we know that $\underline{x}_{i,j} = x_{i \ominus p, j \boxminus q}$ where the symbol $\ominus$ denotes pointwise subtraction in the mixed-radix number system with the invariants of G_1 forming the mixed-radices, and the symbol $\boxminus$ denotes pointwise subtraction in the mixed-radix number system whose mixed radices are the invariants of G_2. Therefore,

$$\begin{aligned}\underline{X}_{k,l} &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} \; \underline{x}_{i,j} \; \bar{h}_n^{l,j} \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} \; x_{i \ominus p, j \boxminus q} \; \bar{h}_n^{l,j} .\end{aligned}$$

Now, put $i \ominus p = r$ and $j \boxminus q = s$.

$$\underline{X}_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,p \oplus r} \; x_{r,s} \; \bar{h}^{l,q \boxplus s} .$$

But, in view of equation A.24 of Appendix A, we may write

$$\bar{h}_m^{k,p \oplus r} = \bar{h}_m^{k,p} \; \bar{h}_m^{k,r} \text{ and } \bar{h}_n^{l,q \boxplus s} = \bar{h}_n^{l,q} \; \bar{h}_n^{l,s}$$

$$\underline{X}_{k,l} = \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} \bar{h}_m^{k,p} \, \bar{h}_m^{k,r} \, x_{r,s} \, \bar{h}_n^{l,q} \, \bar{h}_n^{l,s}$$

$$= \bar{h}_m^{k,p} \, \bar{h}_n^{l,q} \sum_{r=0}^{m-1} \sum_{s=0}^{n-1} \bar{h}_m^{k,r} \, x_{r,s} \, \bar{h}_n^{l,s} \, .$$

Finally, since

$$\sum_{r=0}^{m-1} \sum_{s=0}^{n-1} \bar{h}_m^{k,r} \, x_{r,s} \, \bar{h}_n^{l,s} = X_{k,l}, \text{(from equation 4.1.5)}$$

we have

$$\underline{X}_{k,l} = \bar{h}_m^{k,p} \, \bar{h}_n^{l,q} \, X_{k,l} \, .$$

This completes the proof of the permutation property of the 2-D FDT.

4.2 Transform Domain Description of 2-D P-I Systems

We now present a transform domain description of the 2-D P-I systems. We show that the 2-D FDT satisfies a generalized convolution theorem and that Parseval's theorem applies to 2-D P-I systems. The notion of transfer function for 2-D P-I systems is then introduced and finally the relationship between the transfer characteristics of a given 2-D P-I system and its equivalent 1-D P-I system is examined.

4.2.1 Generalized Convolution Theorem

A generalized convolution theorem for 2-D P-I systems may be stated as follows:

Theorem 4.2.1: The 2-D FDT of the generalized convolution of any two 2-D signals is equal to the pointwise product of the 2-D FDT's of the individual signals.

Thus, if s and x be two 2-D signals and

$y = s * x,$

where $*$ denotes generalized convolution given by (refer to equation 2.4.3)

$$y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{k \ominus i, l \ominus j} \, x_{i,j} \, , \tag{4.2.1}$$

then according to the generalized convolution theorem,

$$Y_{k,l} = S_{k,l} \cdot X_{k,l} \; ; \quad k \varepsilon Z_m, \; l \varepsilon Z_n \, ; \tag{4.2.2}$$

where Y, S and X are the 2-D FDT's of respectively y, s and x, i.e.,

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} \; x_{i,j} \; ; \; \bar{h}_n^{l,j}, k \varepsilon Z_m, l \varepsilon Z_n \, , \tag{4.2.3}$$

$$S_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} \; s_{i,j} \; \bar{h}_n^{l,j} ; \; k \varepsilon Z_m, l \varepsilon Z_n \, , \tag{4.2.4}$$

and $$Y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i}\, y_{i,j}\, \bar{h}_n^{l,j} \quad ; \quad k \varepsilon Z_m, l \varepsilon Z_n \, . \tag{4.2.5}$$

Proof of the generalized convolution theorem: From equations (4.2.1) and (4.2.5) we have

$$Y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i}\, \bar{h}_n^{l,j} \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} s_{i \ominus p, j \boxminus q}\, x_{p,q}$$

$$= \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} x_{p,q} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i}\, s_{i \ominus p, j \boxminus q}\, \bar{h}_n^{l,j}$$

Putting $i \ominus p = r$ and $j \boxminus q = t$,

$i = p \oplus r$ and $j = q \boxplus t$,

$$Y_{k,l} = \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} x_{p,q} \sum_{r=0}^{m-1} \sum_{t=0}^{n-1} \bar{h}_m^{k,p \oplus r}\, s_{r,t}\, \bar{h}_n^{l,q \boxplus t} \, . \tag{4.2.6}$$

But, $\bar{h}_m^{k,p \oplus r} = \bar{h}_m^{k,p}\ \bar{h}^{k,r}$, and

$\bar{h}_n^{l,q \boxplus t} = \bar{h}_n^{l,q}\ \bar{h}_n^{l,t}$ (from equation A.24, Appendix A).

Equation (4.2.6) may be rewritten as

$$Y_{k,l} = \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} x_{p,q} \sum_{r=0}^{m-1} \sum_{t=0}^{n-1} \bar{h}_m^{k,p}\ \bar{h}_m^{k,r}\ s_{r,t}\ \bar{h}_n^{l,q}\ \bar{h}_n^{l,t}$$

$$= \sum_{p=0}^{m-1} \sum_{q=0}^{n-1} \bar{h}_m^{k,p} x_{p,q} \bar{h}_n^{l,q} \sum_{r=0}^{m-1} \sum_{t=0}^{n-1} \bar{h}_m^{k,r} s_{r,t} \bar{h}_n^{l,t} .$$

In view of equations (4.2.3) and (4.2.4), the above equation may be rewritten as

$$Y_{k,l} = S_{k,l} X_{k,l} . \tag{4.2.7}$$

This completes the proof for the generalized convolution theorem.

4.2.2 Parseval's Theorem

Theorem 4.2.2: Let x and y be two 2-D signals belonging to W, the vector space of m x n matrices having entries from C, and let X and Y be the 2-D FDT's of respectively x and y. Then,

$$\sum_{k=0}^{m-1} \sum_{l=0}^{n-1} X_{k,l} \bar{Y}_{k,l} = N \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} \bar{y}_{i,j} \; ; \; N = m.n, \tag{4.2.8}$$

where the bars over $Y_{k,l}$ and $y_{i,j}$ indicate the respective complex conjugates.

Proof:

$$X_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} x_{i,j} \bar{h}_n^{l,j} ,$$

and $$Y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} y_{i,j} \bar{h}_n^{l,j} .$$

Hence,

$$X_{k,l}\,\bar{Y}_{k,l} = \left(\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \bar{h}_m^{k,i}\, x_{i,j}\, \bar{h}_n^{l,j}\right)$$

$$\cdot\left(\sum_{p=0}^{m-1}\sum_{q=0}^{n-1} h_m^{k,p}\, \bar{y}_{p,q}\, h_n^{l,q}\right) ,$$

i.e.,
$$\sum_{k=0}^{m-1}\sum_{l=0}^{n-1} X_{k,l}\,\bar{Y}_{k,l} =$$

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\sum_{p=0}^{m-1}\sum_{q=0}^{n-1}\left(\sum_{k=0}^{m-1} \bar{h}_m^{k,i}\, h_m^{k,p}\right)\left(\sum_{l=0}^{n-1} \bar{h}_n^{l,j}\, h_n^{l,q}\right) x_{i,j}\,\bar{y}_{p,q} .$$

From the orthogonality property of the columns of generalized Hadamard matrices H_m and H_n, we have

$$\sum_{k=0}^{m-1} \bar{h}_m^{k,i}\, h_n^{k,p} = m\,\delta_{i,p} ,$$

and
$$\sum_{l=0}^{n-1} \bar{h}_n^{l,j}\, h_n^{l,q} = n\,\delta_{j,q} .$$

Therefore,

$$\sum_{k=0}^{m-1}\sum_{l=0}^{n-1} X_{k,l}\,\bar{Y}_{k,l} =$$

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\sum_{p=0}^{m-1}\sum_{q=0}^{n-1} (m\,\delta_{i,p})(n\,\delta_{j,q}) x_{i,j}\,\bar{y}_{p,q} =$$

$$N \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} x_{i,j}\,\bar{y}_{i,j} \quad ; \quad N = m.n .$$

4.2.3 Notion of Transfer Function of 2-D P-I Systems

The generalized convolution theorem studied in section 4.2.1 states that the 2-D FDT of the generalized convolution of two 2-D signals s and x equals the pointwise product of the 2-D FDT's of the individual signals s and x. If s and x are now taken to represent respectively the unit response and the input signal of a 2-D P-I system belonging to a certain class, we then have

$$Y_{k,l} = S_{k,l}\, X_{k,l} \quad ; \quad k\varepsilon Z_m,\ l\varepsilon Z_n \, ; \tag{4.2.9}$$

where $Y_{k,l}$, $S_{k,l}$ and $X_{k,l}$ represent the (k,l)-th components of the pertinent 2-D FDT's of respectively the output y, the unit response s and the input x of the system.

The matrix S, having entries $S_{k,l}$, $k\varepsilon Z_m$, $l\varepsilon Z_n$ and obtained as the 2-D FDT of the unit response matrix s of the system, is henceforth said to represent the transfer characteristics of the system under consideration. Since the entries $S_{k,l}$ are in general complex, the matrix S may be specified in terms of two separate matrices $S^{(A)}$ and $S^{(P)}$. Matrix $S^{(A)}$, whose each entry $S^{(A)}_{k,l}$ is the value of the amplitude of the corresponding entry $S_{k,l}$ of S, is said to represent the amplitude characteristics or the amplitude response of the system, while the matrix $S^{(P)}$, whose each entry $S^{(P)}_{k,l}$ is the value of the phase of the corresponding entry $S_{k,l}$

of S, is said to represent the <u>phase characteristics</u> or the <u>phase response</u> of the system. Further, for a 2-D P-I system belonging to a known class and specified in terms of its unit response matrix s, the following equation giving the 2-D FDT of s, viz.,

$$S_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \bar{h}_m^{k,i} \; s_{i,j} \; \bar{h}_n^{l,j} \quad ; \quad k \varepsilon Z_m, \; l \varepsilon Z_n \tag{4.2.10}$$

may be regarded as giving the values of a function $S: Z_m \times Z_n \to C$, and in this sense, it is said to represent the <u>transfer function</u> of that 2-D P-I system.

In particular, when the 2-D P-I system under consideration belongs to the cyclic class, i.e., when the groups G_1 and G_2 relative to which the system is defined are cyclic groups, the 2-D FDT pertaining to this class becomes the 2-D DFT. Thus, for the cyclic class of 2-D P-I systems, the transfer function becomes a function whose values are given by the 2-D DFT of the unit response of the system, i.e.,

$$S_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \gamma_m^{-ki} \; s_{i,j} \; \gamma_n^{-lj} \quad ; \quad k \varepsilon Z_m, \; l \varepsilon Z_n \; ,$$

where γ_m and γ_n are respectively the m-th and the n-th roots of unity and are given by

$$\gamma_m = \exp(\sqrt{-1}\,\frac{2\pi}{m}) \text{ and } \gamma_n = \exp(\sqrt{-1}\,\frac{2\pi}{n}) \, .$$

Then, in terms of the indeterminates or algebraic variables Z_1 and Z_2, the transfer function is explicitly the function

$$S(Z_1,Z_2) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \, Z_1^{-i} \, Z_2^{-j}.$$

As an illustration, if a cyclic 2-D P-I system with a unit response matrix given by

$$s = \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} \\ s_{1,0} & s_{1,1} & s_{1,2} \end{bmatrix}$$

is considered, then

$$S_{k,l} = \sum_{i=0}^{1} \sum_{j=0}^{2} \gamma_2^{-ki} \, s_{i,j} \, \gamma_3^{-lj} = s_{0,0} + s_{0,1} \, \gamma_3^{-l}$$

$$+ s_{0,2} \, \gamma_3^{-2l} + s_{1,0} \, \gamma_2^{-k} + s_{1,1} \, \gamma_2^{-k} \, \gamma_3^{-l} + s_{1,2} \gamma_2^{-k} \, \gamma_3^{-2l},$$

where $\gamma_2 = \exp(\sqrt{-1}\,\frac{2\pi}{2}) = -1$ and $\gamma_3 = \exp(\sqrt{-1}\,\frac{2\pi}{3})$.

Thus, for this cyclic 2-D P-I system, the transfer function is given by

$$S(Z_1,Z_2) = s_{0,0} + s_{0,1} \, Z_2^{-1} + s_{0,2} \, Z_2^{-2} + s_{1,0} \, Z_1^{-1}$$

$$+ s_{1,1} \, Z_1^{-1} \, Z_2^{-1} + s_{1,2} \, Z_1^{-1} \, Z_2^{-2} .$$

Remark 4.2.1: The notion of transfer characteristics and transfer functions, when considered exactly as in the 2-D case, but with respect to a single index, a single transitive abelian permutation group and a single indeterminate, gives the corresponding notions for 1-D P-I systems. They have earlier been used in [1].

4.2.4 Eigenvalues of the 2-D P-I System and Entries of its Transfer Characteristics

The entries of the transfer characteristics, viz., the $S_{k,l}$'s of a given 2-D P-I system T have been defined earlier (section 4.2.3) as the components of the pertinent 2-D FDT of the unit response matrix s of that system. We shall now show that these $S_{k,l}$'s are indeed the eigenvalues of the system T. As we shall see in the next chapter, this point of view will be useful in the discussion on the role of 2-D P-I systems in filtering or spectrum shaping of 2-D signals.

Let T be a 2-D P-I system belonging to a certain class. Let x,y and s belonging to V be respectively its input, output and unit response. Further, let X,Y and S be the pertinent 2-D FDT's of x,y, and s respectively. Then from the generalized convolution theorem we have

$$Y_{i,j} = X_{i,j}\, S_{i,j} \quad ; \quad i \varepsilon Z_m,\ j \varepsilon Z_n .$$

y, the inverse 2-D FDT of Y is given by

$$y = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} Y_{i,j}\, h_N^{i,j} = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, S_{i,j}\, h_N^{i,j}, \tag{4.2.11}$$

where $h_N^{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ is the set of linearly independent orthonormal eigenvectors of the class to which T belongs.

But $y = Tx$,

and $x = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, h_N^{i,j}$.

$$y = Tx = \frac{1}{N} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, T(h_N^{i,j})$$

$$= \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, \sigma_T^{i,j}\, h_N^{i,j}, \tag{4.2.12}$$

where $\sigma_T^{i,j}$ is an eigenvalue of T, the associated eigenvector for it being $h_N^{i,j}$.

From (4.2.11) and (4.2.12) we then have

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}(S_{i,j} - \sigma_T^{i,j})h_N^{i,j} = 0 . \tag{4.2.13}$$

Now, the eigenvectors $h_N^{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ are linearly independent. Hence, we conclude that

$$X_{i,j}(S_{i,j} - \sigma_T^{i,j}) = 0 \text{ for every } i\varepsilon Z_m \text{ and every } j\varepsilon Z_n.$$

But $X_{i,j}$'s, being entries of the 2-D FDT of an arbitrary input signal, are themselves arbitrary, so that we have

$$(S_{i,j} - \sigma_T^{i,j}) = 0 \text{ for every } i\varepsilon Z_m \text{ and every } j\varepsilon Z_n,$$

i.e., $S_{i,j} = \sigma_T^{i,j}$ for every $i\varepsilon Z_m$ and every $j\varepsilon Z_n$.

Thus, we have the following theorem:

Theorem 4.2.2: The entries of the transfer characteristics S of a given 2-D P-I system T which are the components of the pertinent 2-D FDT of the unit response s of that system T, are the eigenvalues of T. Specifically, the (i,j)-th element $S_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ of S is the (i,j)-th eigenvalue of T and has $h_N^{i,j}$, the (i,j)-th eigenvector of T associated with it.

Remark 4.2.2: In view of theorem 4.2.2, we shall henceforth use the same symbol for the system eigenvalues and the entries of the transfer characteristics of a 2-D P-I system.

4.2.5 Relationship Between the Transfer Characteristics of a 2-D P-I System and its 1-D Equivalent

In section 3 of Chapter 3 we had studied the relationship between the unit responses of a 2-D P-I system and its equivalent 1-D P-I system. We will now study the corresponding relationship in the transform domain, i.e., the relationship between the transfer characteristics of a 2-D P-I system and its equivalent 1-D P-I system.

Let the m x n array $S^{(2)}$ be the transfer characteristic of a 2-D P-I system T whose unit response is given by $s^{(2)}$. Then from equation (4.1.3),

$$S^{(2)} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j}^{(2)} \; \overline{h}_N^{i,j}, \tag{4.2.10}$$

where $\overline{h}_N^{i,j}$ is the complex conjugate of the (i,j)-th eigenvector of T.

Now, let t be the 1-D equivalent of T under a linear transformation $Q: V \to R^N$ and let f be the index mapping associated with Q (Chapter 3). If $s^{(1)}$ is the unit sample response vector of t, from equation (3.3.9) we know that

$$s^{(1)} = Q(s^{(2)}), \tag{4.2.11}$$

Therefore, if $(i,j) \to k$ under the index mapping f, then

$$s_{i,j}^{(2)} = s_k^{(1)}, \tag{4.2.12}$$

where $s_{i,j}^{(2)}$ is the (i,j)-th entry of $s^{(2)}$ and $s_k^{(1)}$ is the k-th entry of $s^{(1)}$. Further, the k-th eigenvector of t, viz., H_N^k is given by (refer to equation (3.3.15))

$$H_N^k = Q(h_N^{i,j}) = Q((h_m^i)(h_n^j)^T). \tag{4.2.13}$$

Equation (4.2.10) may be written as

$$S^{(2)} = \sum_{k=0}^{N-1} s_k^{(1)} Q^{-1}(\bar{H}_N^k) = Q^{-1}\left(\sum_{k=0}^{N-1} s_k^{(1)} \bar{H}_N^k\right) = Q^{-1}(S^{(1)})$$

i.e., $S^{(1)} = Q\, S^{(2)}$,

where $S^{(1)}$ is the transfer characteristic vector of t. Thus we have established the following result about the transfer characteristics of 2-D systems and their 1-D equivalents:

Remark 4.2.3: Let T be a 2-D P-I system on V and t on R^N be the 1-D equivalent of T under a linear transformation $Q: V \longrightarrow R^N$. If $S^{(2)}$ and $S^{(1)}$ be the transfer characteristics of the 2-D P-I system T and its 1-D equivalent t, then $S^{(1)} = Q\, S^{(2)}$.

CHAPTER 5

P-I FILTERING OF FINITE DISCRETE 2-D DATA

In Chapter 4 the 2-D FDT was introduced and a transform domain description of 2-D P-I systems was also given. In the present chapter, we first introduce the notion of filtering or spectrum shaping of 2-D signals using 2-D P-I systems and indicate the nature of filter types like low pass, high pass, band pass and band elimination filters with special reference to the cyclic and dyadic classes of 2-D P-I systems. We then consider the notion of separability and study the sample domain as well as transform domain characterization of separable 2-D P-I filters. Finally we give examples illustrating the implementation of separable 2-D P-I filters.

5.1 Notion of Filtering Using 2-D P-I Systems

Let T be a 2-D P-I system on V belonging to a certain class whose eigenvectors are represented by $h_N^{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$. If $S_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ be the set of eigenvalues of T and if the eigenvector $h_N^{i,j}$ be associated with the eigenvalue $S_{i,j}$, then

$$T\, h_N^{i,j} = S_{i,j}\, h_N^{i,j} \;; \quad \text{for every } i\varepsilon Z_m,\ \text{every } j\varepsilon Z_n .$$

Consider an arbitrary 2-D signal $x\varepsilon V$. Then from equation (4.1.4),

$$x = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, h_m^i (h_n^j)^T = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, h_N^{i,j} . \tag{5.1.1}$$

Now, if signal x is given as input to the system T, the resulting output y is given by

$$y = Tx .$$

Substituting for x from equation (5.1.1), we have

$$y = \frac{1}{N}\, T \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, h_N^{i,j} = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, T(h_N^{i,j})$$

$$= \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, S_{i,j}\, h_N^{i,j} .$$

Thus, $y = T(x) = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, S_{i,j}\, h_N^{i,j}$ (5.1.2)

while, $x = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} X_{i,j}\, h_N^{i,j}.$ (5.1.3)

Equations (5.1.2) and (5.1.3) show precisely the way the spectrum of a signal x gets altered in passing through the system T. Each spectral coefficient $X_{i,j}$ of the input signal gets changed into a spectral coefficient $S_{i,j}\, X_{i,j}$ at the output, the $S_{i,j}$'s being the eigenvalues of the system T, or equivalently the entries of the transfer characteristics of T. The process of passing a signal through a system to produce such an effect on the spectrum is commonly referred to as filtering or spectrum shaping of a finite discrete 2-D signal $x \epsilon V$. In keeping with this nomenclature, a 2-D P-I system is here called a 2-D P-I filter if the process of convolving a finite discrete 2-D signal with its unit response produces the desired modifications in the spectrum of the signal. It may be noted that just as the filtering performed by LTI systems is with respect to the complex exponentials which are the eigensignals of those systems, in the present case the filtering is with respect to the eigenvectors of the pertinent class to which the 2-D P-I system T belongs. In particular, if T belongs to the cyclic class, the filtering is with respect to discrete complex exponentials and is termed as Fourier domain 2-D P-I filtering.

On the other hand, if T belongs to the dyadic class of 2-D P-I P-I systems, the filtering is then with respect to discrete Walsh functions and this filtering is called Walsh domain 2-D P-I filtering.

In the case of 2-D cyclic P-I filters which perform 2-D Fourier domain filtering, the pertinent eigenvectors are $h_m^i(h_n^j)^T$, $i\varepsilon Z_m$, $j\varepsilon Z_n$, h_m^i and h_n^j being given by

$$h_m^i = (1\ \gamma_m^i\ \gamma_m^{2i}\ldots\ \gamma_m^{\alpha i}\ldots\ \gamma_m^{(m-1)i})^T \ ;\ \alpha,\ i\varepsilon Z_m,$$

and $$h_n^j = (1\ \gamma_n^j\ \gamma_n^{2j}\ldots\ \gamma_n^{\beta j}\ldots\ \gamma_n^{(n-1)j})^T \ ;\ \beta,\ j\varepsilon Z_n,$$

where $\gamma_k = \exp(\sqrt{-1}\ \frac{2\pi}{k})$.

Thus, h_m^i and h_n^j, $i\varepsilon Z_m$, $j\varepsilon Z_n$ are vectors with discrete complex exponentials as their entries. In keeping with the general practice [38] the integral index i of h_m^i (and similarly j of h_n^j) will be called frequency.

In the case of the 2-D dyadic P-I filters which perform 2-D Walsh domain filtering, the pertinent eigenvectors are $W_N^{i,j} = w_m^i(w_n^j)^T$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ where w_m^i and w_n^j denote respectively the i-th column of the sequency-ordered Walsh-Hadamard matrix H_m of order m and the j-th column of the sequency-ordered Walsh-Hadamard matrix H_n of order n; since we are dealing with the dyadic case, m and n must be some integer powers of 2. Therefore w_m^i and w_n^j are vectors with discrete Walsh functions as their entries and for which [39] the integral index i of w_m^i (or the j of w_n^j) is referred to as the sequency.

Classification of 1-D P-I filters of the cyclic or dyadic class as low pass, high pass, band pass and band elimination filters is based on the fact that the pertinent eigen signals for the 1-D case involve only one frequency or sequency variable and so can be ordered in increasing order of frequency or sequency. In the 2-D case, however, two frequency or sequency variables are involved and hence classification of 2-D cyclic and dyadic P-I filters into types like low pass, high pass, band pass and band elimination filters can be done in several possible ways. Fig. 5.1 shows what are called the rectangular ideal amplitude characteristics of 2-D cyclic P-I filters of these various types. Ideal rectangular transfer characteristics of 2-D dyadic P-I filters of various types are shown in Fig. 5.2. In these figures, a pass band is that portion of the amplitude characteristics $A_{k,l}$, $k \varepsilon Z_m$, $l \varepsilon Z_n$, where $A_{k,l}$ is greater than a prescribed value and a stop band is that portion where $A_{k,l}$ is less than a prescribed value. It may be observed that the amplitude characteristics of the cyclic class exhibit an even symmetry. This symmetry arises from the fact that the entries of the unit response matrix are real [40].

Implementation of 2-D P-I filtering may be either explicitly in the transform domain or in the sample domain.

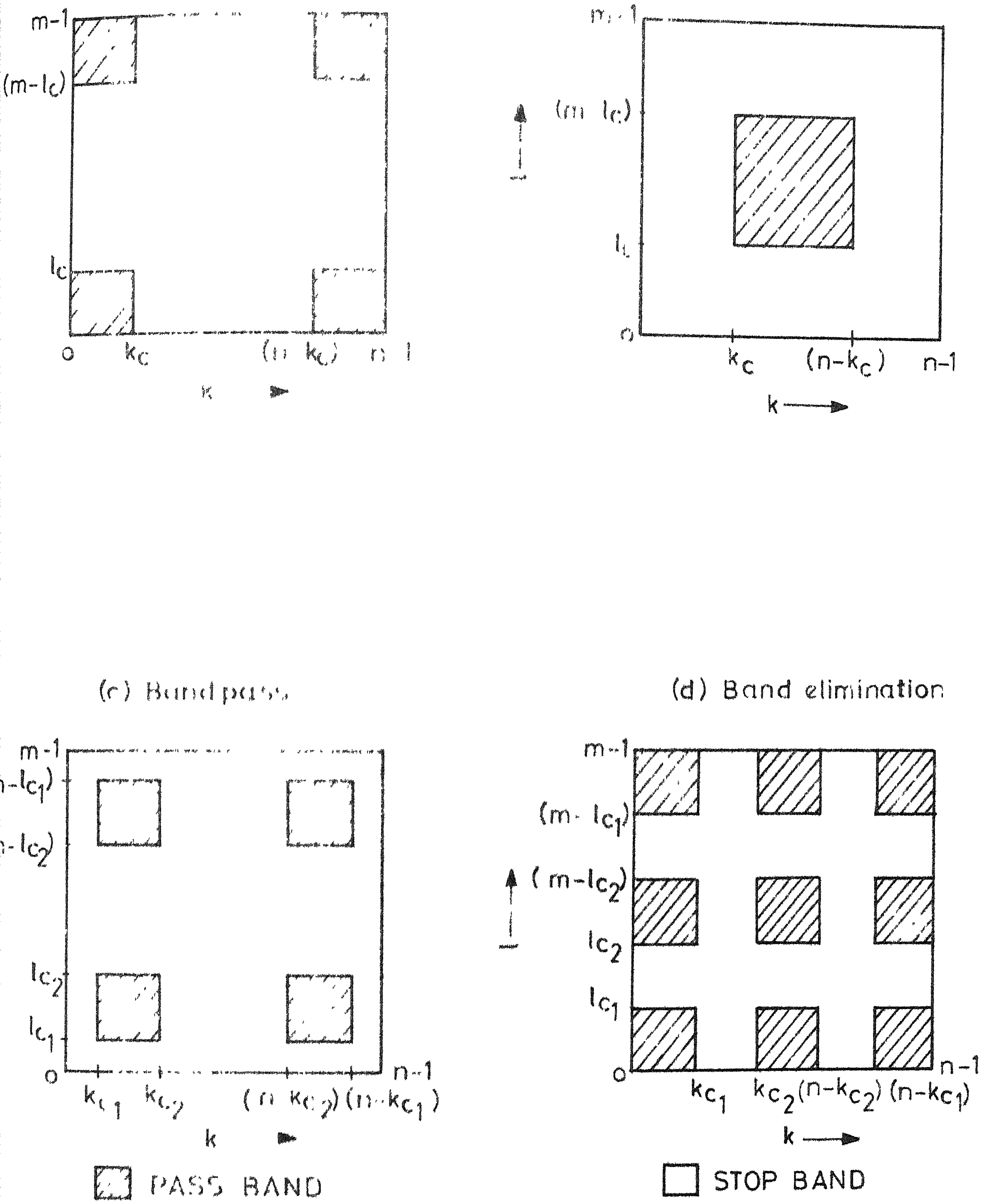


FIG.5.1 IDEAL RECTANGULAR AMPLITUDE CHARACTERISTICS OF CYCLIC 2-D P-I FILTERS

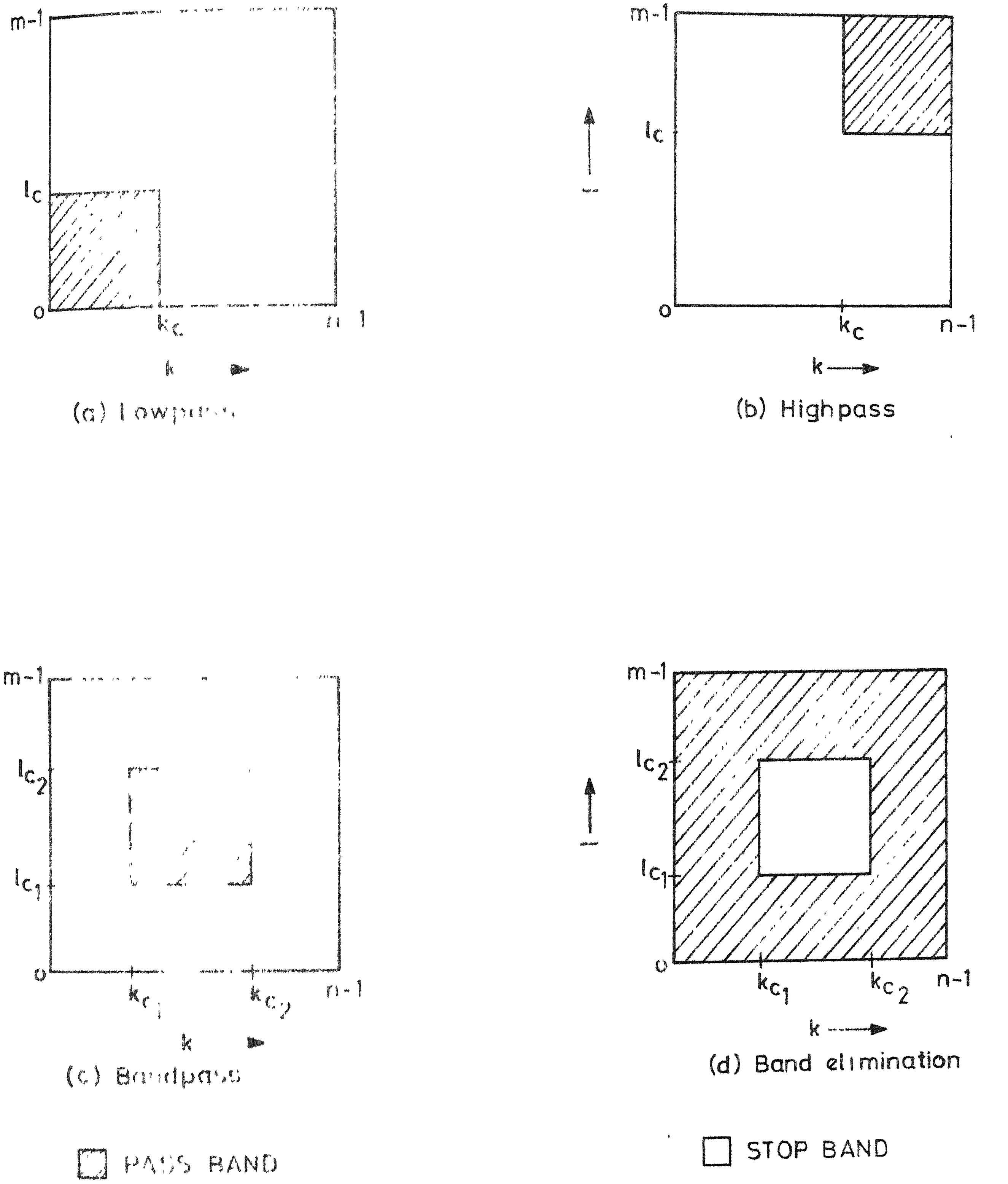


FIG. 5.2 IDEAL RECTANGULAR AMPLITUDE CHARACTERISTICS OF DYADIC 2-D P-I FILTERS

The transform domain implementation is based on the transform domain characterization of the 2-D P-I filter, viz.,

$$Y_{k,l} = S_{k,l}\, X_{k,l} \quad ; \quad k\varepsilon Z_m,\ l\varepsilon Z_n.$$

This implementation consists of three steps in cascade : (i) taking the 2-D FDT $X_{k,l}$ of the 2-D signal x, (ii) multiplying in a pointwise manner the 2-D FDT coefficients $X_{k,l}$, $k\varepsilon Z_m$, $l\varepsilon Z_n$ of x by the corresponding entries $S_{k,l}$, $k\varepsilon Z_m$, $l\varepsilon Z_n$ of the desired transfer characteristics of the filter, and finally, (iii) taking the inverse 2-D FDT of the resulting array. If the 2-D P-I filter is of the cyclic (or dyadic) class, steps (i) and (iii) are generally carried out using 2-D fast Fourier transform (or 2-D fast Walsh transform) techniques.

The sample domain implementation is based on the convolutional relationship.

$$y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{k \ominus i,\, l \boxminus j}\; x_{i,j} \quad ; \quad k\varepsilon Z_m,\ l\varepsilon Z_n$$

and consists of executing the various arithmetical operations involved in this convolution, through appropriate computational algorithms.

5.2 Separable 2-D P-I Filters

The question of using 1-D techniques for processing 2-D data was discussed earlier in Chapter 3 and it was shown there that every 2-D P-I system has an equivalent 1-D P-I system which makes possible the conversion of 2-D filtering problems into exactly equivalent 1-D filtering problems in so far as finite discrete data are concerned. While this equivalence provides a general method, a more straightforward application of 1-D techniques to 2-D tasks arises in cases where the specified ideal transfer characteristics of a 2-D P-I system are of what is known as the separable type.

Definition 5.2.1: The transfer characteristics of a 2-D P-I system T defined relative to G_1 and G_2 of orders respectively m and n, are said to be separable if the transfer characteristics matrix S can be represented as

$$S = S^1(S^2)^T, \tag{5.2.1}$$

so that S^1 may be treated as the transfer characteristic vector of some 1-D P-I system H_1 of dimension m defined relative to G_1 and S^2 as the transfer characteristic vector of some other 1-D P-I system H_2 of dimension n defined relative to G_2. A 2-D P-I system with separable transfer characteristics, is said to be separable.

The above definition of separable 2-D P-I systems is transform domain oriented. A corresponding sample domain definition of separability easily follows. Let s be the unit response matrix of the 2-D P-I system T and let s_1 and s_2 be the unit response vectors of the 1-D P-I systems H_1 and H_2 respectively mentioned in definition 5.2.1. Then

$$S = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \bar{h}_m^i (\bar{h}_n^j)^T$$

$$S^1 = \sum_{i=0}^{m-1} s_1^i \bar{h}_m^i \quad ; \quad \text{and}$$

$$S^2 = \sum_{j=0}^{n-1} s_2^j \bar{h}_n^j \; .$$

It then follows from definition of separability that

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{i,j} \bar{h}_m^i (\bar{h}_n^j)^T = (\sum_{i=0}^{m-1} s_1^i \bar{h}_m^i)(\sum_{j=0}^{n-1} s_2^j \bar{h}_n^j)^T$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_1^i s_2^j \bar{h}_m^i (\bar{h}_n^j)^T,$$

i.e., $$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (s_{i,j} - s_1^i s_2^j) \bar{h}_m^i (\bar{h}_n^j)^T = 0 \; . \qquad (5.2.2)$$

Since the eigenvectors $h_m^i (h_n^j)^T$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ of T are linearly independent, equation (5.2.2) implies that

$$s_{i,j} = s_1^i \, s_2^j \text{ for every } i \varepsilon Z_m, \text{ every } j \varepsilon Z_n$$

or, equivalently that

$$s = s_1 \, (s_2)^T \tag{5.2.4}$$

It is seen by reversing the arguments that (5.2.4) implies (5.2.1). Thus,

<u>Theorem 5.2.1</u>: A 2-D P-I system T defined relative to the groups G_1 of order m and G_2 of order n is separable iff its unit response matrix s can be represented as

$$s = s_1 \, (s_2)^T,$$

where s is the unit sample response vector of a 1-D P-I system H_1 of dimension m defined relative to the group G_1 and s_2 is the unit sample response vector of another 1-D P-I system H_2 of dimension n defined relative to the group G_2.

5.2.1 Representing Separable 2-D P-I Systems in terms of P-I Matrices

A separable 2-D P-I system T has a simple representation in terms of P-I matrices as we shall presently see. If T has a unit response matrix s, then

$$s \stackrel{d}{=} T_{0,0} = s_1 \, (s_2)^T.$$

But s_1 and s_2, being the unit sample response vectors

of 1-D P-I systems H_1 and H_2 respectively, are the zeroth columns $H_1^{(0)}$ and $H_2^{(0)}$ of the corresponding system matrices H_1 and H_2 respectively ; i.e.,

$$s_1 = H_1^{(0)} \text{ and } s_2 = H_2^{(0)}. \tag{5.2.5}$$

Therefore,

$$s \overset{d}{=} T_{0,0} = H_1^{(0)} \, (H_2^{(0)})^T .$$

The standard response matrices $T_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ of the system T are given by (refer to section 2.1)

$$\begin{aligned} T_{i,j} &= p_i \, T_{0,0} \, q_j^T = p_i \, H_1^{(0)} (H_2^{(0)})^T \, q_j^T \\ &= (p_i \, H_1^{(0)})(q_i \, H_2^{(0)})^T \quad ; \quad p_i \varepsilon G_1 ; \; i\varepsilon Z_m ; \; q_i \varepsilon G_2 , j\varepsilon Z_n . \end{aligned} \tag{5.2.6}$$

But $p_i \, H_1^{(0)} = H_1^{(i)}$, the i-th column of the system matrix H_1, and $q_j \, H_2^{(0)} = H_2^{(j)}$, the j-th column of the system matrix H_2.

Therefore, equation (5.2.6) may be written as

$$T_{i,j} = H_1^{(i)} \, (H_2^{(j)})^T .$$

But $T_{i,j}$'s being standard response matrices of T, for any 2-D signal $x\varepsilon V$, we have,

$$Tx = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} \, T_{i,j} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{i,j} \, H_1^{(i)} (H_2^{(j)})^T$$

or, $\quad Tx = H_1 \, x \, H_2^T .$

Thus it has been shown that if T is a separable 2-D P-I system defined relative to G_1 and G_2 of orders m and n respectively, then T is given by the explicit relation

$$Tx = H_1 \, x \, H_2^T , \qquad (5.2.7)$$

where H_1 and H_2 are m x m and n x n P-I matrices representing 1-D P-I systems defined relative to G_1 and G_2 respectively.

On the other hand, if a 2-D P-I system T is given by the relation (5.2.7) then as we shall presently see, it is a separable 2-D P-I system.

Let δ_i denote the m x 1 vector $(0,0,\ldots, 1,0,\ldots,0)^T$ in which the i-th entry alone is a 1 and all the other entries are zeros, and δ_j denote the m x 1 vector $(0,0,\ldots,1,0,\ldots,0)^T$ in which j-th entry alone is a 1 and all other entries are zeros. Then the standard response matrix $T_{i,j}$, $i\varepsilon Z_m$, $j\varepsilon Z_n$ may be written,

$$T_{i,j} = T \, \Delta_{i,j} = H_1 \, \Delta_{i,j} \, H_2^T = H_1 \, \delta_i \, \delta_j^T \, H_2^T$$

$$= (H_1 \, \delta_i)(H_2 \, \delta_j)^T.$$

Since $H_1 \, \delta_i = H_1^{(i)}$, the i-th column of H,

$$T_{i,j} = H_1^{(i)} \, (H_2^{(j)})^T.$$

Thus,

$$s = T_{0,0} = H_1^{(0)} \, (H_2^{(0)})^T = s_1 \, (s_2)^T .$$

Then from theorem 5.2.1, it follows that T is a separable 2-D P-I system. Thus we have fully established the following result:

Theorem 5.2.2: A 2-D P-I system T defined relative to G_1 of order m and G_2 of order n is separable iff it can be characterized by a relation

$$Tx = H_1 \, x \, H_2^T ,$$

Where H_1 and H_2 are m x m and n x n P-I matrices representing 1-D P-I systems defined relative to G_1 and G_2 respectively.

5.2.2 Convolutional Characterization of Separable 2-D P-I Systems

The generalized convolutional relationship for 2-D P-I systems derived in Chapter 2 takes a simple and interesting form in the case of separable 2-D P-I systems. If s is the unit response matrix of a separable 2-D P-I system T relative to G_1 of order m and G_2 of order n, then from theorem 5.2.1,

$$s_{k,l} = s_1^k \;\; s_2^l , \qquad (5.2.8)$$

Where $s_{k,l}$ is the k,l-th entry of s, s_1^k is the k-th entry of the unit sample vector of a 1-D P-I system H_1 defined

relative to G_1 and s_2^l is the l-th entry of the unit sample vector of a 1-D P-I system H_2 defined relative to G_2.

The generalized convolutional relationship for 2-D P-I systems was shown to be given by (refer to equation 2.4.3).

$$y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_{k \ominus i,\, l \boxminus j}\, x_{i,j}\,, \tag{5.2.9}$$

where $y_{k,l}$ is the (k,l)-th entry of the output signal and $x_{i,j}$ is the (i,j)-th entry of the input signal, $\ominus$ denotes subtraction operation in the mixed-radix number system with the invariants of group G_1 as mixed radices and $\boxminus$ denotes subtraction operation in the mixed-radix number system with the invariants of group G_2 as the mixed radices.

In view of equation (5.2.8), the generalized convolutional relationship given by equation (5.2.9) may be written as

$$y_{k,l} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} s_1^{k \ominus i}\, s_2^{l \boxminus j}\, x_{i,j}\,,$$

$$\text{i.e.,} \quad y_{k,l} = \sum_{i=0}^{m-1} s_1^{k \ominus i} \sum_{j=0}^{n-1} s_2^{l \boxminus j}\, x_{i,j}\,. \tag{5.2.10}$$

Equation (5.2.10) shows that the 2-D convolution represented by equation (5.2.9) may equivalently be obtained through 1-D convolutions. In other words, the output y may be obtained in two steps;(i) convolving s_2 with each one of the rows

of x to get a partially filtered output 2-D signal $\bar{y}$, and (ii) ~~then~~ convolving each column of $\bar{y}$ with s_1 to get the final filtered output y.

The steps outlined above lead to the exact sample domain implementation of a separable 2-D P-I filter. It is clear that unless the input signal size, i.e., m x n is small the storage requirements and the computational effort involved would be considerable. However, approximate implementations, involving reasonable storage and computational time requirements which give good approximations to the desired transfer characteristics, are possible. For example, the desired ideal transfer characteristic vectors S^1 and S^2 may each be approximated in the least-squares sense. For the case when S is a zero phase transfer characteristic, if s_1 of length m and s_2 of length n are the unit sample response vectors corresponding to S^1 and S^2 respectively, then such a least-squares approximation of S^1 and S^2 can be obtained by retaining only say p entries of s_1 and q entries of s_2 such that $p < m$ and $q < n$.

To illustrate the implementation scheme outlined above for the separable 2-D P-I filters, we consider two filtering examples, one in the Fourier domain and the other in the Walsh domain.

Example 5.2.1: A low pass zero phase cyclic 2-D P-I filter with $m = 48$, $n = 48$ and specified ideal rectangular transfer characteristics having cutoff frequencies $k_c = 10$ and $l_c = 10$ is to be implemented. Pass band amplitude response $= 1.0$ and stop band amplitude response is zero.

We shall use least-sequares approximation by using an 8-term approximation for each of the sample response vectors s_1 and s_2 . These 8 sample response coefficients to be used have been computed and are given in Table 5.1.

Table 5.1: Sample Response Coefficients in Example 5.2.1

i	s_1^i and s_2^i
0	0.39583
1	0.30163
2	0.09716
3	-0.05933
4	-0.07775
5	-0.00424
6	0.05030
7	0.03106

Entries of the approximate transfer characteristics of the 1-D cyclic P-I systems H_1 and H_2 obtained under the 8-term

approximation of the sample response vectors s_1 and s_2, are tabulated in Table 5.2. In this table, only the first 24 entries are shown because of the even symmetry of the transfer characteristics S^1 and S^2.

Table 5.2: Entries of the Approximate Transfer Characteristic Vectors of H_1 and H_2 in Example 5.2.1

i	S_i^1 , S_i^2	i	S_i^1 , S_i^2
0	1.07350	12	0.05459
1	1.03957	13	0.06738
2	0.96691	14	0.02206
3	0.91991	15	0.02067
4	0.94615	16	0.02990
5	1.03398	17	0.01178
6	1.11173	18	-0.00906
7	1.09089	19	-0.01464
8	0.92412	20	-0.00584
9	0.63843	21	0.00432
10	0.32164	22	0.00584
11	0.07204	23	0.00043

The realized transfer characteristics of the 2-D cyclic P-I filter are shown in Fig. 5.3.

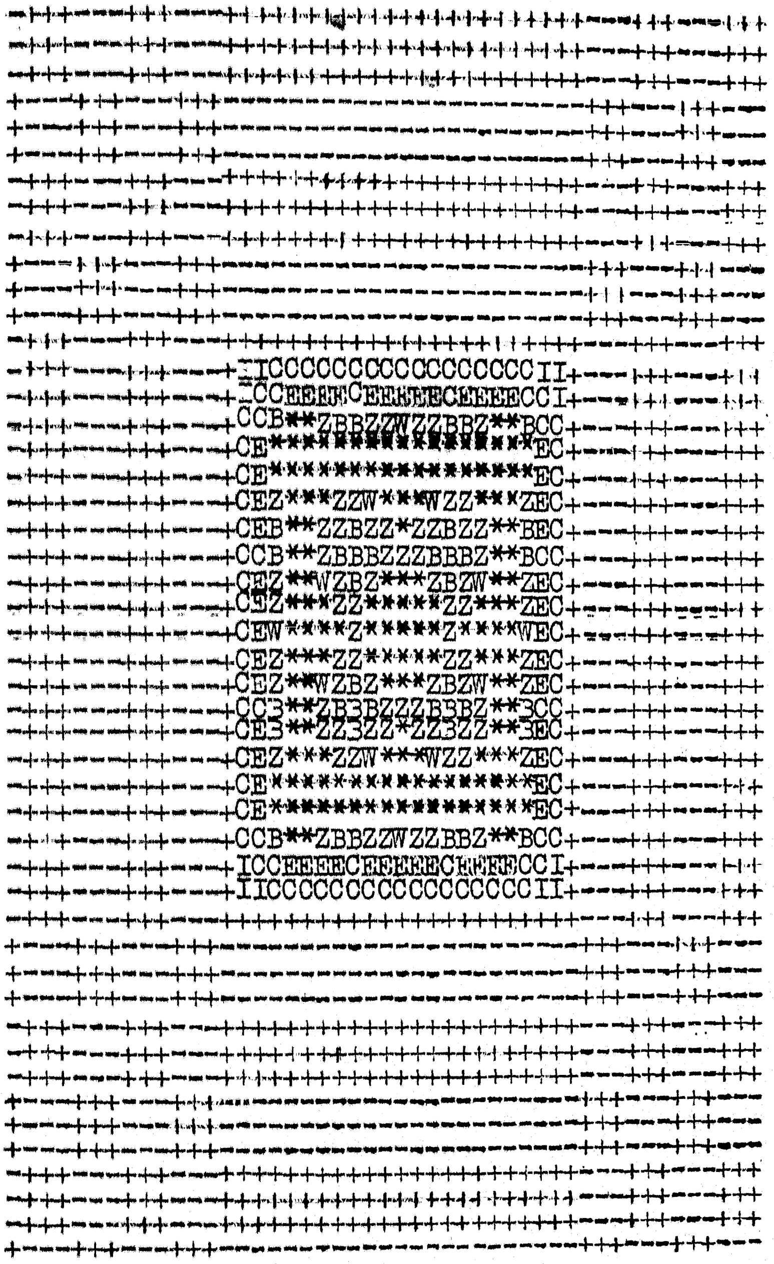


Fig. 5.3: Realized Amplitude Characteristics of the ~~2-D~~ Cyclic 2-D P-I Filter in Example 5.2.1.

*	1.13	B	0.89	I	0.39
W	1.00	E	0.79	+	0.09
Z	0.99	C	0.59	-	-0.04

Example 5.2.2: A dyadic 2-D P-I filter with m = n = 32 and specified ideal rectangular amplitude characteristics having cutoff sequencies $k_c = 7$ and $l_c = 15$ is to be implemented. The pass band amplitude response is 1.0 and stop band amplitude response is zero.

Least-squares approximation is obtained with 8-term sample response vectors s_1 and s_2 for the 1-D P-I systems H_1 and H_2. The entries of s_1 and s_2 are tabulated in Table 5.3.

Table 5.3: Sample Response Coefficients in Example 5.2.2

i	s_2^i	s_1^i
0	0.46875	0.21875
1	0.46875	0.21875
2	0.03125	0.21875
3	0.03125	0.21875
4	-0.03125	0.03125
5	-0.03125	0.03125
6	0.03125	0.03125
7	0.03125	0.03125

The realized transfer characteristics for this 2-D dyadic filter are shown in Fig. 5.4.

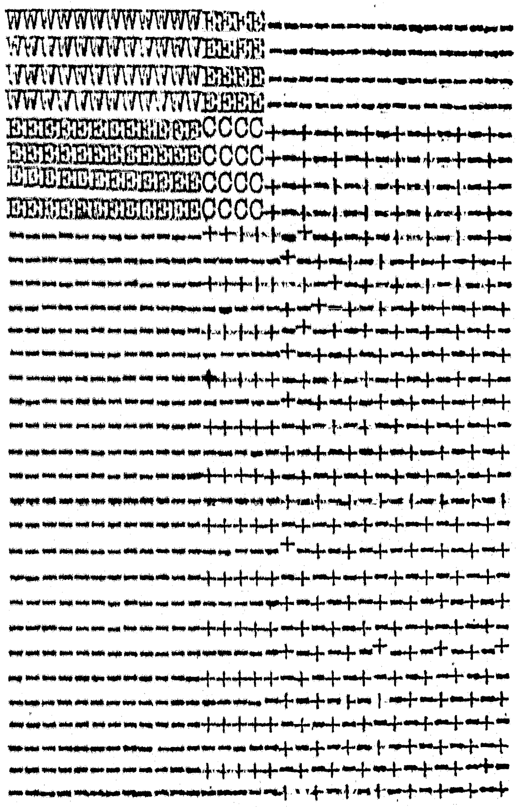


Fig. 5.4: Realized Amplitude Characteristics of the Dyadic 2-D P-I Filter in Example 5.2.2.

*	1.13	C	0.59
W	1.00	I	0.39
Z	0.99	+	0.09
B	0.89	-	-0.04
E	0.79		

5.3 Multistage Separable Realization

Separability of a 2-D P-I system (see definition 5.2.1) may equivalently be stated in terms of the rank of its transfer characteristics matrix or its unit response matrix. It may be recalled [41,p.92] that a matrix S of size m x n is expressible in the form

$$S = S^1 \quad (S^2)^T$$

where, S^1 and S^2 are column vectors of sizes m x 1 and n x 1 respectively, if and only if S is of rank 1. Then, in view of the definition of separability and theorem 5.2.1 it follows that a 2-D filter is separable if and only if the ranks of its unit response matrix as well as its transfer characteristics matrix are 1. The observation is often helpful in determining whether the desired filter is directly realizable in separable form or not. As an example, consider the ideal rectangular characteristics shown in Figs. 5.1 and 5.2 in which we assume that the response is 1 in the pass band and zero in the stop band. Inspection of the rows of these characteristics reveals that there is only one linearly independent row in each of them. It, therefore, follows they are both of the separable type. In contrast, it may be verified that the ideal circularly symmetric lowpass transfer characteristics are not separable, there being more than 1 linearly independent rows in such characteristics.

A filter which is not by itself in a separable form may, as a compromise, be realized as a linear combination of several separable filters. This possibility is based on the following result [41 ,p.93] concerning transformations on finite dimensional vector spaces:

Lemma 5.3.1: If A is a linear transformation of rank k on a finite dimensional vector space, then A may be written as the sum of k transformations of rank one.

From this lemma, it immediately follows that if the rank of the specified unit response matrix of a 2-D filter is, say, k, then it can be realized as a cascade of k stages of separable filters since its unit response matrix can be written as

$$S = \alpha_1 S_1 + \alpha_2 S_2 + \cdots\cdots + \alpha_k S_k .$$

In this expression, S_i is the response matrix of the i-th separable filter expressible in the form

$$S_i = S_i^1 (S_i^2)^T .$$

Such a realization of a 2-D P-I filter may be seen to be the P-I counterpart of the multistage separable realization of LTI digital filters proposed by Shanks and Treitel [7].

CHAPTER 6

IMPLEMENTATION OF 2-D P-I SYSTEMS IN TERMS OF THEIR EQUIVALENT 1-D P-I SYSTEMS

In Chapter 5 the problem of applying 1-D techniques to the filtering of finite discrete 2-D data was considered in terms of the special case wherein the specified 2-D transfer characteristics were separable. In this chapter, we adopt a different approach to the problem. To be specific, we consider here a method of 1-D implementation of 2-D P-I filters which is based on the results obtained in Chapter 3 pertaining to the equivalence between 2-D and 1-D P-I systems. This method permits the use of 1-D techniques for 2-D tasks irrespective of whether the specified 2-D transfer characteristics are separable or not. As shown here the exact 1-D equivalent of a dyadic 2-D P-I system is again a dyadic P-I system while the exact 1-D equivalent of a cyclic 2-D P-I system is cyclic provided a minor restriction on the frame size of the pertinent 2-D

signal array is satisfied. Thus, this method is particularly suitable in dealing with problems concerning filtering of finite discrete 2-D data in the Fourier and Walsh domains, especially, when the specified 2-D transfer characteristics are not separable. In view of this, only cyclic and dyadic classes of P-I systems are considered in this chapter.

Given a 2-D P-I system T on V, the space of real m x n matrices, in order to obtain its 1-D equivalent, we need to use an appropriate linear transformation $Q: V \to R^N$, or equivalently, an appropriate index mapping $f: Z_m \times Z_n \to Z_N$, $N = m.n.$ The choice of the index mapping has to take into account the composition of the group G relative to which the equivalent 1-D P-I system is defined. It may be noted here that the choice of the index mapping determines only the structure of the permutation matrices constituting the group G but not the composition of this group. The composition of the group G is governed by the fact that G is isomorphic to the direct product of G_1 and G_2 (refer to Theorem 3.3.1) where G_1 and G_2 constitute the pair of groups relative to which the given 2-D P-I system has been defined. We examine the nature of these direct product groups separately for the two specific cases wherein the two groups G_1 and G_2 are (i) cyclic, and (ii) dyadic. We first take up the case of cyclic filters in the following section.

6.1 Implementation of a Cyclic 2-D P-I System Through its 1-D Equivalent

Filtering of finite discrete 2-D data in the Fourier domain corresponds to cyclic 2-D P-I filtering. This means that the 2-D filter required to perform filtering in this domain will be permutation invariant relative to two cyclic groups G_1 and G_2. Therefore, its 1-D equivalent will be permutation-invariant relative to a group of permutation matrices G which is isomorphic to the direct product of two cyclic groups G_1 and G_2. We will now examine the composition of this direct product group.

6.1.1 Direct Product of Cyclic Groups

A standard result in group theory [29, p.12] is that a direct product $H_1 \times H_2 \times \ldots \times H_r$ of cyclic groups is cyclic if and only if their orders $\{h_i\}$ are powers of distinct primes.

When this result is applied to the problem of obtaining the 1-D equivalent t of a 2-D P-I system T on V, it follows that the group G relative to which t is permutation-invariant, is a cyclic group iff m and n which are respectively the orders of the two cyclic groups G_1 and G_2 (relative to which T is defined), are relatively prime. Since m and n also represent respectively, the number of rows and columns of

the arrays in the signal space V of T, it follows that

<u>Theorem 6.1.1</u>: If T be a 2-D cyclic P-I system, then its equivalent 1-D system t is a P-I system belonging to a cyclic class iff the number of rows m and the number of columns n of the pertinent input signals of T are relatively prime.

Thus, two cases arise depending upon whether m and n are relatively prime or not. We will now consider the implications of each one of these cases with reference to our ultimate objective of implementing a 2-D cyclic P-I system in terms of its equivalent 1-D P-I system.

a. <u>m and n not relatively prime</u>: Referring to Theorem 6.1.1 we know that in this case the equivalent 1-D P-I system is not a cyclic one. This means that the well established design procedures available for cyclic convolutional systems cannot be made use of for this equivalent 1-D P-I system. So, we will not discuss this case any further.

b. <u>m and n are relatively prime</u>: In this case the equivalent 1-D P-I system is cyclic making it possible to rely on the well developed design techniques available for cyclic convolutional systems. Further, a specified transfer function of a 2-D cyclic P-I system which involves two frequency variables, can in this case be reduced with the help of a suitable one-to-one index mapping $f: Z_m \times Z_n \rightarrow Z_N$, into a transfer function involving only one frequency variable, the resulting transfer function being that of the equivalent 1-D

P-I system obtained under the index mapping f. Moreover, the condition that m, the number of rows, and n, the number of columns, should be relatively prime is, infact, only a minor restriction on the frame size of the input signals. Since m and n need not themselves be prime numbers, a wide range of choice is still available for m and n and, if need be, they can be made almost equal while keeping them mutually prime. Therefore, in our study of equivalent 1-D implementation of 2-D cyclic P-I systems, we shall henceforth assume that m and n are relatively prime.

6.1.2 Equivalent 1-D Implementation of 2-D Cyclic P-I Systems

As a first step in the implementation of a 2-D cyclic P-I system T in terms of its equivalent 1-D cyclic P-I system t, we now choose an appropriate one-to-one index mapping $f\colon Z_m \times Z_n \to Z_N$. If G be the cyclic group relative to which t is permutation-invariant, an appropriate index mapping for the cyclic case is chosen here by requiring that the matrix members of G, constructed as outlined in Chapter 3 (refer to section 3.2), get ordered according to increasing powers of the generator of G. As shown here, when the matrix members of G are ordered in this manner, they assume the form of cyclic permutation matrices with respect to the standard basis of R^N, so that the available theory of cyclic

convolutional systems can be directly applied to the equivalent 1-D cyclic P-I system.

Let T be a 2-D cyclic P-I system relative to G_1 and G_2 of orders m and n respectively, where m and n are relatively prime. Let p and q denote the permutation matrices of size m x m and n x n respectively, that are the generators of G_1 and G_2. Since G_1 and G_2 are cyclic groups, with the usual scheme of ordering [App.A] members of transitive abelian permutation groups, the i-th member of G_1, $i \varepsilon Z_m$ is p^i and the j-th member of G_2, $j \varepsilon Z_n$, is q^j. If the system t is a 1-D equivalent of T obtained under a linear transformation Q: $V \to R^N$ then, as shown in Chapter 3, it is permutation-invariant relative to the cyclic group G of permutation matrices $p^i \otimes_Q q^j$, $i \varepsilon Z_m$, $j \varepsilon Z_n$. With p and q as the generators of G_1 and G_2 respectively, the generator of the cyclic group G is $p \otimes_Q q$ so that if we order the matrix elements of G in the order of increasing powers of this generator, the k-th element of G is given by $P_k = (p \otimes_Q q)^k$. Now, if the one-to-one index mapping f associated with the linear transformation Q (remark 3.1.1) maps the pair of integers (i,j) into the integer k, i.e., if

$$f(i,j) = k \quad ; \quad i \varepsilon Z_m, \; j \varepsilon Z_n, \; k \varepsilon Z_N,$$

then the elements of the group G will be ordered according

to increasing powers of its generator provided, the index mapping f is such that

$$P_k = (p^i \otimes_Q q^j) = (p \otimes_Q q)^k \text{ for every } k \epsilon Z_N . \qquad (6.1.1)$$

From standard properties of Kronecker product of matrices,

$$(p \otimes_Q q)^k = p^k \otimes_Q q^k . \qquad (6.1.2)$$

But p is the generator of the cyclic group of order m so that $p^m = I_m$, where I_m is the m x m identity matrix. Similarly, $q^n = I_n$, where I_n is the n x n identity matrix. Therefore, with $k \epsilon Z_N$ where $N = m.n$, equation (6.1.2) may be rewritten as

$$(p \otimes_Q q)^k = (p^{(k)_m} \otimes_Q q^{(k)_n}),$$

no ( )$_n$ in the equation

where $(k)_r$ denotes the residue of k modulo r. Thus, equation (6.1.1) becomes

$$P_k = (p^i \otimes_Q q^j) = (p^{(k)_m} \otimes_Q q^{(k)_n}) \text{ for every } k \epsilon Z_n . \qquad (6.1.3)$$

In other words, the index mapping f should be such that equation (6.1.3) is true for every $k \epsilon Z_N$. For such an index mapping

$$\left.\begin{aligned} & f(i,j) = k \\ & k \equiv i \bmod m, \text{ and} \\ & k \equiv j \bmod n . \end{aligned}\right\} ; \quad k \epsilon Z_N,\ i \epsilon Z_m,\ j \epsilon Z_n \qquad (6.1.4)$$

Note that, since m and n are ~~mutually~~ relatively prime, the Chinese Remainder Theorem (CRT) provides a unique solution for k in terms of i and j. Thus, this index mapping is one-to-one.

This mapping f orders the matrix members of the group G (relative to which the equivalent 1-D P-I system t is defined) according to increasing powers of its generator P so that the k-th member of this group, denoted by P_k, is given by

$$P_k = p^i \otimes_Q q^j = P^k,$$

where (i, j) is the ordered pair of integers mapped onto k by f.

Next we show that the matrix members of G assume the form of cyclic permutation matrices when this index mapping is used. For this purpose all that we need to show is that the generator P of G is a cyclic permutation matrix which has a 1 only in the $(r + 1)_N$-th row and r-th column position for any $r \varepsilon Z_N$. This follows from the fact that this index mapping orders members of G according to increasing powers of its generator P. First let us consider the zeroth row of P separately. This corresponds to r = N-1 so that this row should have a 1 only in the (N-1)-th column position. To see that it is indeed so, recall the way the matrix members of G are constructed. The zeroth row of P denoted by $P^{(0)}$ is obtained

by taking the Kronecker product of the zeroth row of p, the generator of G_1 and the zeroth row of q, the generator of G_2, treating these row vectors as (1 x m) and (1 x n) matrices. Therefore,

$$P^{(0)} = p^{(0)} \otimes_Q q^{(0)}, \qquad (6.1.5)$$

where $p^{(0)}$ and $q^{(0)}$ are the zeroth rows of the cyclic matrices p and q. From the properties of cyclic permutation matrices, we know that $p^{(0)}$ has a 1 only in the (m-1)-th column position and zeros everywhere else, and that $q^{(0)}$ has a 1 only in the (n-1)-th column position. Then, from (6.1.5) it follows that $P^{(0)}$ will have a 1 only in the u-th column position where u = f((m-1), (n-1)). This means that u is the unique solution of the simultaneous congruences

$$u \equiv (m-1) \bmod m,$$

and $$u \equiv (n-1) \bmod n.$$

It is easy to verify that u = (N-1), where N = m.n, is a solution of these simultaneous congruences because ((N-1)-(m-1)) is divisible by m and ((N-1)-(n-1)) is divisible by n. Since m and n are mutually prime, the above simultaneous congruences have a unique solution and therefore, u = (N-1) is that solution. Thus, the zeroth row of P has a 1 in the (N-1)-th column position and nowhere else.

To examine the structure of the other rows of P, consider in general the v-th row of P where, $1 \leq v \leq (N-1)$. If P is a cyclic permutation matrix, its v-th row should have a 1 only in the (v-1)-th column position. Let

$$f^{-1}(v) = (i,j)$$

so that

$$\begin{aligned} i &= (v)_m, \text{and} \\ j &= (v)_n . \end{aligned} \tag{6.1.6}$$

Then, $$P^{(v)} = p^{(i)} \otimes_Q q^{(j)} = p^{((v)_m)} \otimes_Q q^{((v)_n)}; \tag{6.1.7}$$

where $P^{(v)}$ is the v-th row of P, and $p^{((v)_m)}$ and $q^{((v)_n)}$ are respectively the $(v)_m$-th and $(v)_n$-th rows of p and q. Since $p^{((v)_m)}$ has a 1 only in the $((v)_m-1)$-th column position and $q^{((v)_n)}$ has a 1 only in the $((v)_n-1)$-th column position, then from equation (6.1.7) it follows that $P^{(v)}$ will have a 1 in the w-th position and zeros elsewhere, where

$$w = (((v)_m-1), ((v)_n-1)). \tag{6.1.8}$$

But from equation (6.1.6) we have

$$v = (i,j) = ((v)_m, (v)_n),$$

so that

$$(v-1) = ((v-1)_m, (v-1)_n) = (((v)_m-1), ((v)_n-1)) = w,$$

i.e., $w = (v-1)$,

Thus, the v-th row, $1 \leq v \leq (N-1)$, of P viz., $P^{(v)}$ will have a 1 in the (v-1)-th column position and zeros elsewhere. Therefore, P, the generator of G is a N x N cyclic permutation matrix of the form

$$\begin{bmatrix} 0 & 0 & \cdots\cdots\cdots & 0 & 1 \\ 1 & 0 & \cdots\cdots\cdots & 0 & 0 \\ 0 & 1 & \cdots\cdots\cdots & 0 & 0 \\ 0 & 0 & \cdots\cdots\cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots\cdots\cdots & 1 & 0 \end{bmatrix}.$$

With the generator P assuming this form, all the other members of G also assume the form of cyclic permutation matrices since they are powers of this generator. Thus, when an index mapping of the form (6.1.4) is used, the cyclic group G of permutation matrices has its members ordered according to increasing powers of its generator and further, all the members of G assume the form of cyclic permutation matrices.

Having chosen an appropriate index mapping, we shall next see how the transfer characteristics of the equivalent 1-D system can be obtained from the specified 2-D transfer characteristics. It may be recalled from Chapter 4 (remark 4.2.2) that the transfer characteristics vector $S^{(1)}$ of an equivalent 1-D P-I system is related to the transfer characteristics array $S^{(2)}$ of the 2-D P-I system by the relation

$$S^{(1)} = Q\, S^{(2)},$$

where Q is the linear transformation which is used for obtaining the equivalent 1-D system. This equivalently means that the entries of $S^{(1)}$, viz., $S_k^{(1)}$, $k \varepsilon Z_N$ may be written down from the entries of $S^{(2)}$, viz., $S_{i,j}^{(2)}$, $i \varepsilon Z_m$, $j \varepsilon Z_n$ using the relation

$$S_k^{(1)} = S_{i,j}^{(2)} \quad , \text{ where } (i,j) = f^{-1}(k),$$

f being the one-to-one index mapping associated with the transformation **Q** (remark 3.1.1). $S_k^{(1)}$, which is the k-th eigenvalue of the equivalent 1-D P-I system, is associated with the k-th eigenvector of t given by

$$H_N^k = Q(h_m^i (h_n^j)^T) = h_m^i \otimes_Q h_n^j \,.$$

At this stage, a point about the frequency ordering of the eigenvectors ought to be noted. In the case of cyclic P-I systems with which we are concerned in this section, the eigenvectors H_N^k will not in general be obtained in the natural frequency order for values of k equal to 0,1,2,..., (N-1) in that order. When the index mapping described by equation (6.1.4) is used for obtaining the equivalent 1-D system t, the frequency, p, of the k-th eigenvector of t is given by the formula [32,33].

$$p = (mi + nj) \bmod N \;; \quad 0 \leq p < N \;;\; N = m.n\,. \qquad (6.1.9)$$

It may be mentioned here that the mapping of indices given by (6.1.4) and the frequency mapping given by equation (6.1.9) have been in use in connection with the multidimensional formulation of DFT [32,33]We are using them here in the converse role for the purpose of obtaining 1-D implementation of a given 2-D cyclic P-I filter.

The 2-D requirements, given in the form of 2-D transfer characteristics, may now be translated into corresponding 1-D requirements in the form of 1-D transfer characteristics in the natural frequency order. When in this form, the transfer characteristics are called here as frequency ordered 1-D transfer characteristics. A 1-D cyclic P-I filter with its transfer characteristics approximating those of the frequency ordered 1-D transfer characteristics which are obtained from the specified 2-D characteristics may now be implemented using a suitable approximation technique. For the purpose of illustrating the equivalent 1-D implementation of a given 2-D cyclic P-I filter, we now consider the following example in which for convenience we use the least-squares approximation technique:

Example 6.1.1: A zero phase 2-D cyclic P-I filter with input signals of frame size 51 x 49 and specified circularly symmetric ideal low pass transfer characteristics as shown in Fig. 6.1 is to be implemented.

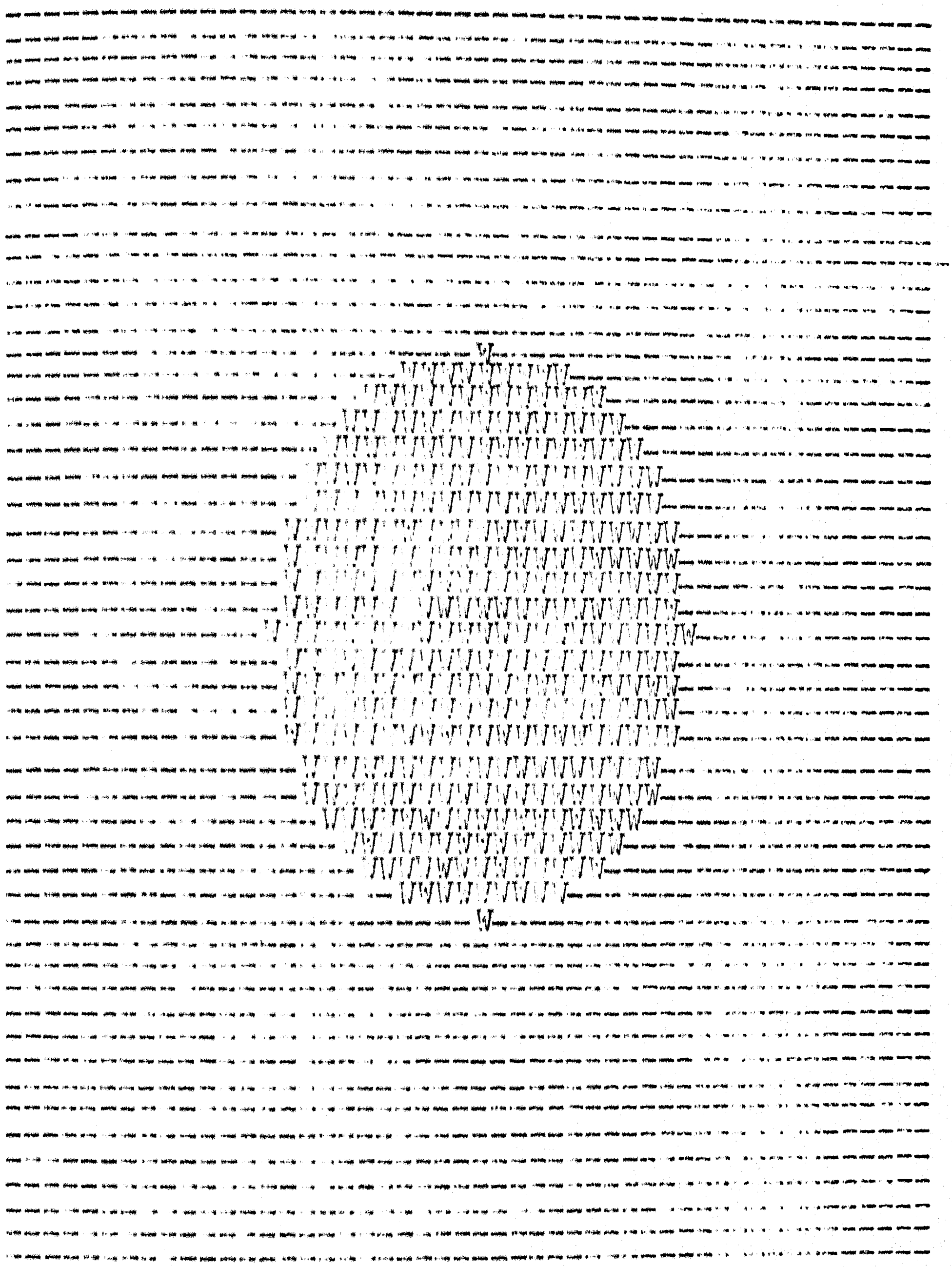


Fig. 6.1: Specified Amplitude Characteristics of the 2-D P-I Filter in Example 6.1.1.

W 1.00

\- 0.00

This 2-D filter is implemented in terms of its 1-D equivalent under a linear transformation $Q: V \rightarrow R^N$ corresponding to an index mapping of the form given by equation (6.1.4) using the values $m = 51$ and $n = 49$. As a first step, the frequency ordered transfer characteristics vector of its 1-D equivalent under Q is obtained from the specified ideal 2-D transfer characteristics, using the frequency relationship given by equation (6.1.9). The unit sample response vector of a 1-D cyclic P-I filter of length 51 x 49 = 2499, which approximates this ideal frequency ordered 1-D transfer characteristics vector in the least squares sense, is then obtained by retaining only the first 312 terms of the inverse DFT of the ideal frequency ordered transfer characteristics vector and assuming zeros for the rest, keeping its even symmetry in mind [1]. Sample domain implementation of the equivalent 1-D cyclic P-I filter then consists of cyclically convolving this unit sample response vector with the equivalent 1-D signal obtained from a given 2-D input signal under the transformation Q. Finally, the filtered version of the given 2-D input signal is obtained by using the inverse transformation Q^{-1}. The given 2-D P-I filter has been implemented using this procedure and the realized 2-D transfer characteristics are shown in Fig. 6.2. The entries of the unit sample response of the equivalent 1-D system are not tabulated here in view of the large number of terms involved.

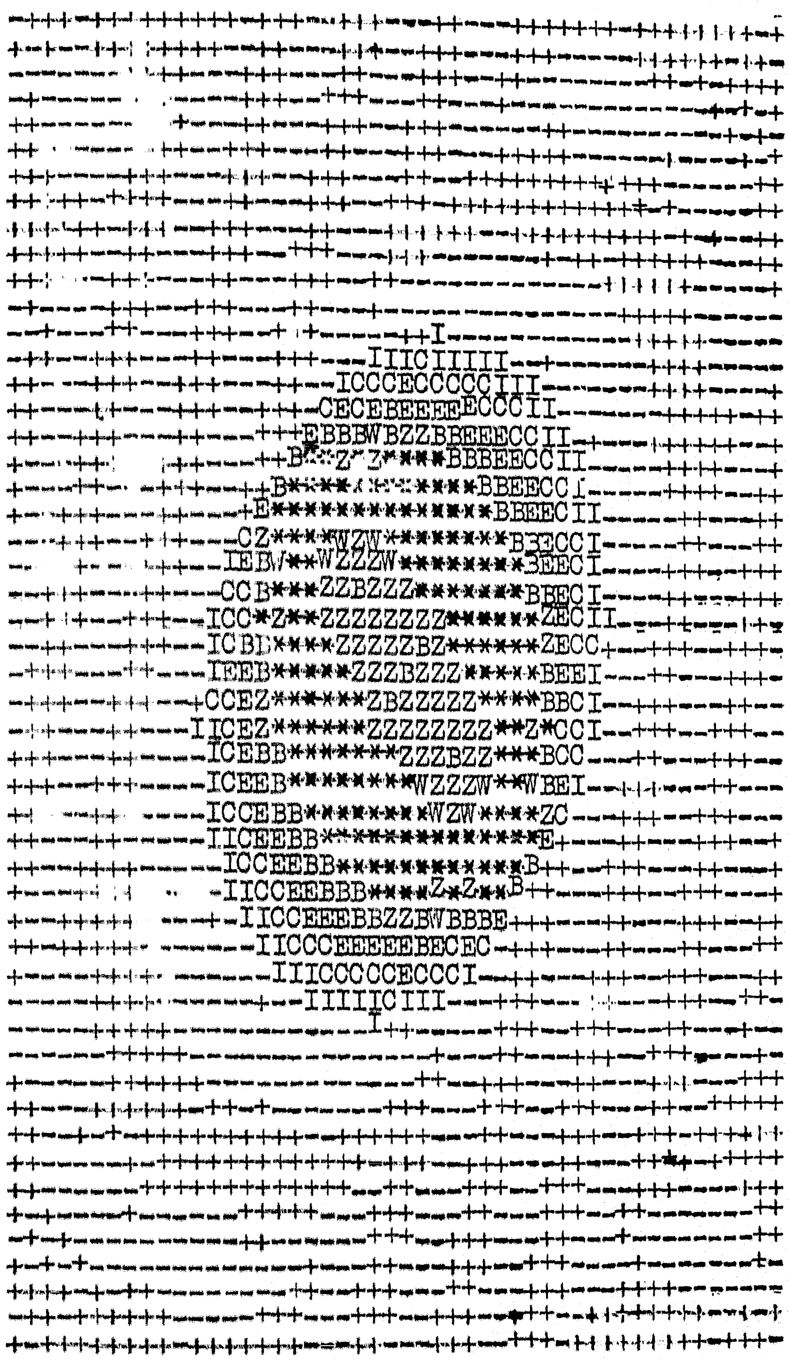


Fig. 6.2: Realized Amplitude Characteristics of the Cyclic 2-D P-I Filter of Example 6.1.1.

*	1.13	B	0.89	I	0.39
W	1.00	E	0.79	+	0.09
Z	0.99	C	0.59	-	-0.04

In the next example, we implement a 2-D cyclic P-I notch filter. The equivalent 1-D cyclic P-I filter is in this case implemented as a recursive digital filter designed to have the appropriate transfer characteristics.

Example 6.1.2: A 2-D P-I notch filter with input signals of frame size 13 x 14 is to be implemented. Its amplitude response is to be zero at frequencies (8,7) and (5,7) and unity elsewhere.

Let t be the 1-D equivalent of the desired 2-D cyclic P-I notch filter under a linear transformation Q that corresponds to an index mapping of the form given by equation (6.1.4). We first obtain the frequency ordered amplitude response characteristics of t from the specified 2-D requirements by using the frequency formula given in equation (6.1.9). In these frequency ordered response characteristics, the zero response frequencies are thus found to be 21 and 161, corresponding respectively to the zero response frequencies (8,7) and (5,7) specified for the 2-D filter. These ideal frequency ordered amplitude characteristics of t, the equivalent 1-D cyclic P-I filter, are then approximated by a transfer function of the following form:

$$H(Z) = \frac{a_0 + a_1 Z^{-1} + a_0 Z^{-2}}{1 + b_1 Z^{-1} + b_2 Z^{-2}} \qquad (6.1.10)$$

Here, the coefficients a_0, a_1, b_1 and b_2 are so chosen that the poles of H(Z) are within the unit circle, and in addition, the amplitude response is zero at a frequency of 21, and is unity at frequencies 0 and 91. Coefficient values determined on this basis are given below:

$$a_0 = 0.599561$$
$$a_1 = -0.8986220$$
$$b_1 = -0.898845$$
$$b_2 = 0.1994225.$$

If H(Z) in equation (6.1.10) is interpreted as the transfer function of a digital filter, the sample domain description of this filter is then

$$y(n) + b_1 y(n-1) + b_2 y(n-2) =$$
$$a_0 x(n) + a_1 x(n-1) + a_0 x(n-2), \qquad (6.1.11)$$

with x(n) and y(n) denoting the n-th input and output samples respectively.

The steady state output of this digital filter for a periodic input of 182 samples per period, is the same as that of the cyclic P-I filter, t, whose transfer function is represented by equation (6.1.10), the input signal vector to the cyclic P-I filter being constituted by the 182 samples in one period of the input sequence given to the digital filter.

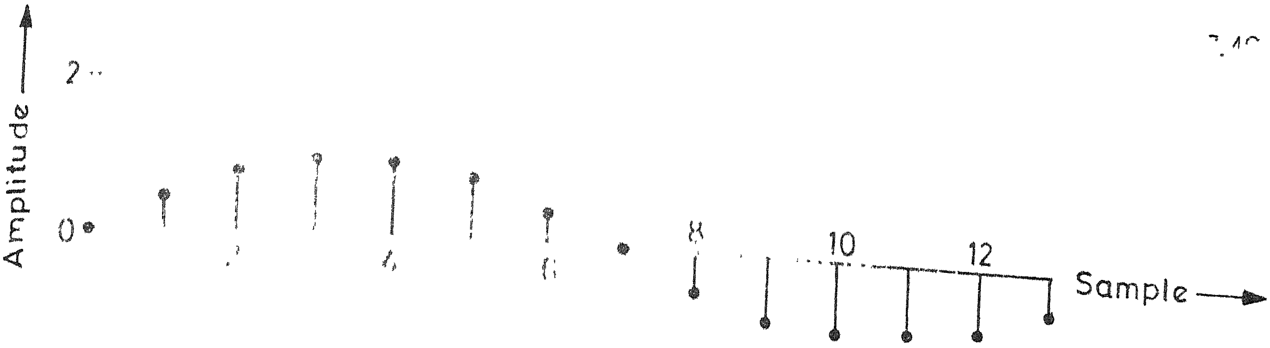
This fact was utilized for computer simulation and the 1-D P-I filtering was carried out by implementing the recursive algorithm (6.1.11) of the digital filter, the input fed to it being that sequence whose one period was the 1-D equivalent of the 2-D finite discrete signal which was to be filtered. It may be noted that this approach of simulation provides a link between the theories of 1-D digital filters (characterized by linear convolutions) and cyclic P-I filters.

For this implementation, the 2-D finite discrete signal which is to be filtered, is taken to be the sum of two components - X_d, a desired signal and X_n, a noise signal. These are given by

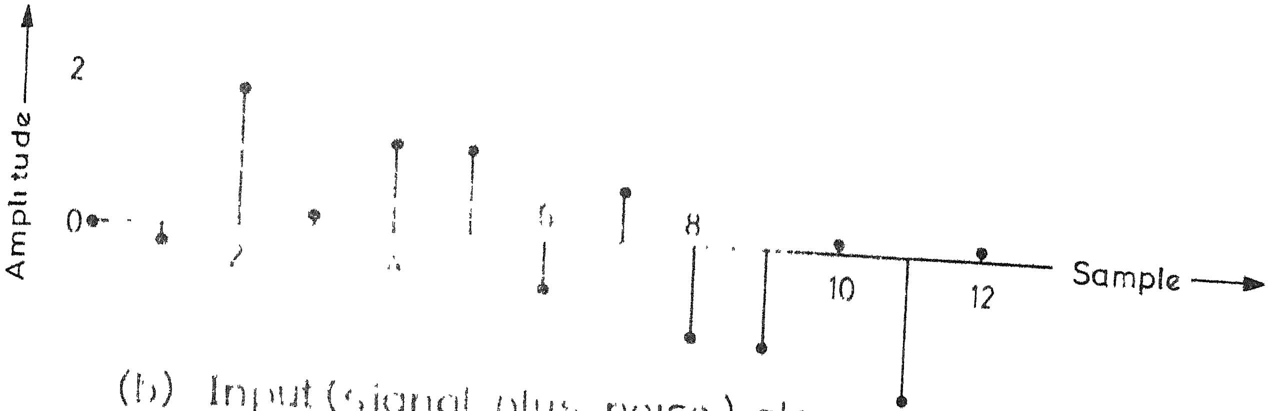
$$X_d = \mathrm{Sin}\left(\frac{2\pi}{13} i + \frac{2\pi}{14} j\right) \quad ; \quad i\varepsilon Z_{13} \; ; \; j\varepsilon Z_{14} \,, \text{ and}$$

and $$X_n = \mathrm{Sin}\left(\frac{16\pi}{13} i + \pi j\right) \quad ; \quad i\varepsilon Z_{13} \; ; \; j\varepsilon Z_{14} \,.$$

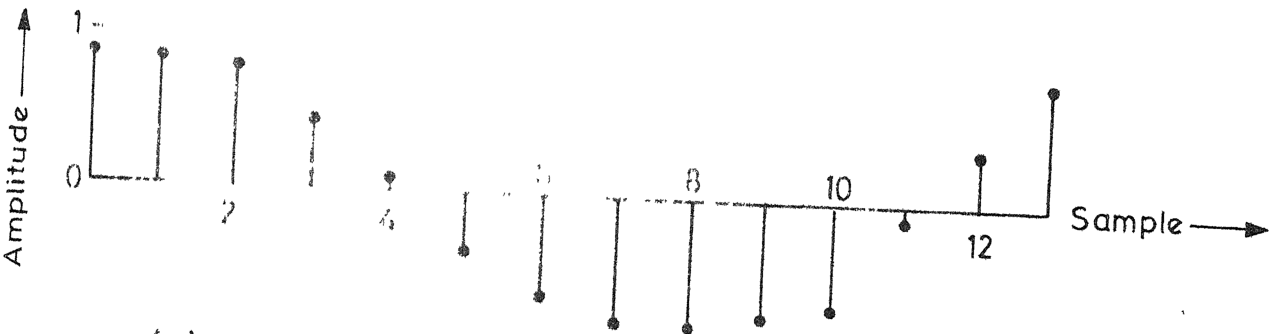
The noise signal X_n, a double sinusoid corresponding to the specified notch frequency for the 2-D filter, is eliminated in the output. In Fig. 6.3, (a) and (b) show respectively the first row and first column of the 2-D input signal while (c) and (d) show respectively the first row and first column of the output 2-D signal.



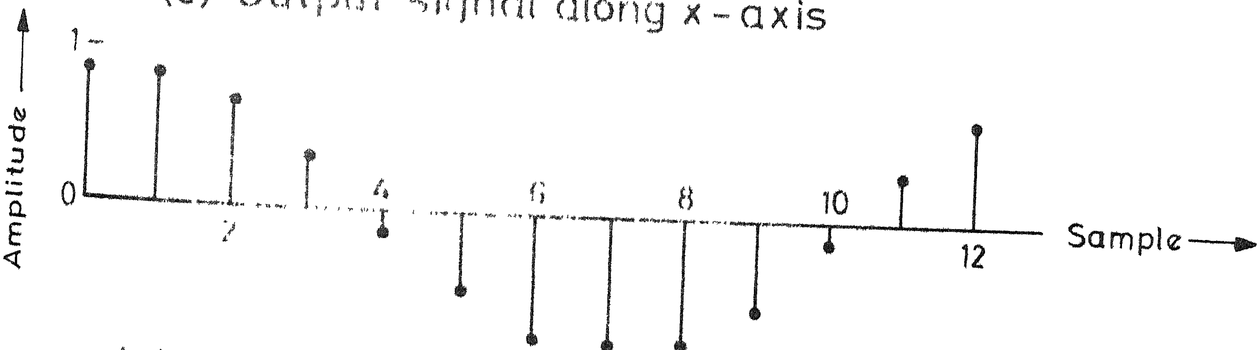
(a) Input (signal plus noise) along x-axis



(b) Input (signal plus noise) along y-axis



(c) Output signal along x-axis



(d) Output signal along Y-axis

FIG. 6.3 INPUT AND OUTPUT SIGNALS OF CYCLIC 2-D P-I NOTCH FILTER IN EXAMPLE 6.1.2

6.2 Implementation of a Dyadic 2-D P-I System Through its 1-D Equivalent

Filtering of finite discrete 2-D data in the Walsh domain corresponds to dyadic 2-D P-I filtering. In other words, a 2-D filter required to perform filtering in this domain is permutation-invariant relative to two dyadic groups G_1 and G_2. Then, from the results in Chapter 3 we know that its 1-D equivalent is permutation-invariant relative to a group of permutation matrices G which is isomorphic to the direct product of the two dyadic groups G_1 and G_2. We shall now examine the nature of this direct product group.

6.2.1 Direct Product of Dyadic Groups

It is known that a group G_1 with invariants m_α, $\alpha \varepsilon Z_{r_1}$, is isomorphic to the direct product of r_1 cyclic groups g_0, g_1, ... , g_{r_1-1} with invariants m_0, m_1, ... , m_{r_1-1} respectively. Now, if we assume G_1 to be a dyadic group of order 2^{r_1}, we know that its invariants $m_\alpha, \alpha \varepsilon Z_{r_1}$ are each equal to 2. Therefore,

$$G_1 \doteq g_0 \times g_1 \times g_2 \times \dots \times g_{r_1-1} . \qquad (6.2.1)$$

In equation (6.2.1), the symbol $\doteq$ is used to mean 'is isomorphic to', and g_i, $i \varepsilon Z_{r_1}$ are all cyclic groups, each of order 2. But then a cyclic group of order 2 is isomorphic to a dyadic group of order 2. Therefore,

$$G_1 \doteq D_2 \times D_2 \times \ldots \times D_2 \qquad (r_1 \text{ factors}), \qquad (6.2.2)$$

where D_2 is a dyadic group of order 2.

Now, if G_2 is a dyadic group of order 2^{r_2}, it can be expressed according to equation (6.2.2) as the direct product of r_2 dyadic groups each of order 2. It then follows that the direct product of G_1 and G_2 is a dyadic group of order $2^{r_1+r_2}$. Hence we make the following remarks:

Remark 6.2.1: The direct product of dyadic groups is dyadic.

Remark 6.2.2: Unlike the cyclic case, here there is no restriction on the orders of G_1 and G_2 for their direct product to be a dyadic group. Hence, for convenience, we shall assume both of them to have the order n. This equivalently means that the signal arrays for the 2-D dyadic P-I systems are assumed to have n rows and n columns.

6.2.2 Equivalent 1-D Implementation of 2-D Dyadic P-I Systems

It follows from remark 6.2.1 that if T is a 2-D dyadic P-I system, then its equivalent 1-D system t is also a dyadic P-I system. Now, to choose an appropriate index mapping in this case, we follow a procedure which is essentially the same as the one we adopted for the cyclic case. Thus, we require the index mapping in the present case to be such

that the matrix members of the dyadic group G, relative to which the equivalent 1-D system is permutation-invariant, assume the standard form of dyadic permutation matrices with respect to the standard basis in R^N, $N = n^2$. With members of G in this form, it will be possible to directly apply the existing theory of dyadic convolution systems for the design and implementation of the equivalent 1-D dyadic system. Following a procedure similar to the one used in the cyclic case, we conclude that the index mapping we are seeking in the present case is the one corresponding to the familiar lexicographic ordering of pairs of indices, i.e.,

$$f(i,j) = k = (ni + j) \quad ; \quad i,j \varepsilon Z_n, \; N = n^2, \; k \varepsilon Z_N . \tag{6.2.3}$$

Now, using a linear transformation Q which corresponds to this index mapping, it is possible to obtain the 1-D equivalent, t, of a given 2-D dyadic P-I system T, when the latter is specified in the sample domain. But if the 2-D P-I system is specified in terms of its transfer characteristics, it is necessary to obtain corresponding specifications for the equivalent 1-D system. The transfer characteristics of the equivalent 1-D system may be obtained by the relation (refer to remark 4.2.2)

$$S^{(1)} = Q \, S^{(2)}, \tag{6.2.4}$$

where $S^{(1)}$ denotes the transfer characteristics vector of the equivalent 1-D system and $S^{(2)}$ denotes the specified transfer characteristics matrix of the 2-D P-I system.

As was pointed out in section 6.1.2 in connection with the 1-D implementation of 2-D cyclic P-I filters, the transfer characteristics vector of the equivalent 1-D system obtained through equation (6.2.4) will not in general be sequency ordered. As pointed out there, if $f(i,j) = k$ where f is the index mapping given by equation (6.2.3), then, in order to arrive at the sequency ordered transfer characteristic of the equivalent 1-D system, what we need to know is the sequency value corresponding to this k. We examine this question in the following section.

6.2.3 Sequency-Ordered Transfer Characteristics of the Equivalent 1-D System

Let

$$S^{(2)} = \begin{bmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,n-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,n-1} \\ \vdots & \vdots & & \vdots \\ s_{n-1,0} & s_{n-1,1} & \cdots & s_{n-1,n-1} \end{bmatrix}$$

be the specified transfer characteristics matrix of T, a 2-D

dyadic P-I system. Since we are considering a dyadic system, n must be a power of 2. So let

$$n = 2^r, \tag{6.2.5}$$

where r is some positive integer. Let

$$S^{(2)} = \begin{bmatrix} s_{0,0} & s_{0,1} & \cdots\cdots & s_{0,n-1} \\ s_{1,0} & s_{1,1} & \cdots\cdots & s_{1,n-1} \\ \vdots & \vdots & & \vdots \\ s_{n-1,0} & s_{n-1,1} & \cdots\cdots & s_{n-1,n-1} \end{bmatrix}$$

be the unit response matrix of T. Then

$$S^{(2)}_{k,l} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{k,i} \; s^{(2)}_{i,j} \; h_n^{l,j} \quad ; \; k,l\varepsilon Z_n \, , \tag{6.2.6}$$

where $h_n^{k,i}$ is the (k,i)-th element of the n-th order Hadamard matrix (sequency ordered) and given by

$$h_n^{k,i} = \prod_{\alpha=0}^{r-1} (-1)^{k_{r-1-\alpha}(i_\alpha + i_{\alpha+1})} . \tag{6.2.7}$$

Here, k_β and i_β are digits in the binary expansion of the integers k and i respectively.

Let $S^{(1)}$ denote the sequency ordered transfer characteristics vector of the equivalent 1-D system obtained under a transformation Q corresponding to the index mapping given by equation (6.2.3). Then its m-th entry is given by

$$S_m^{(1)} = \sum_{p=0}^{N-1} h_N^{m,p}\, s_p^{(1)} \quad ; \quad m\varepsilon N \, , \qquad (6.2.8)$$

Here, $h_N^{m,p}$ is the (m,p)-th element of the N-th order Hadamard matrix (sequency ordered), and is given by

$$h_N^{m,p} = \prod_{\beta=0}^{2r-1} (-1)^{m_{2r-1-\beta}(p_\beta + p_{\beta+1})} \, . \qquad (6.2.9)$$

Now, let

$$\left.\begin{aligned} f^{-1}(p) &= (i,j) \\ \text{and} \quad f^{-1}(m) &= (t,u) \end{aligned}\right\} , \qquad (6.2.10)$$

where f is the index mapping given by equation (6.2.3). Since f is a lexicographic mapping, (i,j) and (t,u) are the representations of p and m respectively, with respect to the fixed radix n. The binary representation of p is therefore obtained by concatenating the binary representations of i and j,

i.e., $(p_{2r-1}, p_{2r-2}, \dots , p_r, p_{r-1}, p_{r-2}, \dots , p_0) =$

$$(i_{r-1}, i_{r-2}, \dots , i_0, j_{r-1}, j_{r-2}, \dots\dots , j_0) \qquad (6.2.11)$$

Hence, from equations (6.2.9) and (6.2.10) we have,

$$h_N^{m,p} = \{ \prod_{\beta=0}^{r-1} (-1)^{m_{2r-1-\beta}(p_\beta + p_{\beta+1})} \} \times$$

$$\{ \prod_{\beta=0}^{2r-1} (-1)^{m_{2r-1-\beta}(p_\beta + p_{\beta+1})} \}$$

$$= \{ (-1)^{m_{2r-1}(p_0 + p_1)} . (-1)^{m_{2r-2}(p_1 + p_2)} \ldots$$

$$(-1)^{m_{2r-1-(r-1)}(p_{r-1} + p_r)} \} \times$$

$$\{ (-1)^{m_{2r-1-r}(p_r + p_{r+1})} . (-1)^{m_{2r-1-(r+1)}(p_{r+1}+p_{r\cdot}}$$

$$\ldots\ldots (-1)^{m_{2r-1-(2r-1)}(p_{2r-1})} \}.$$

Using equation (6.2.10),

$$h_N^{m,p} = \{(-1)^{m_{2r-1}(j_0 + j_1)} . (-1)^{m_{2r-2}(j_1 + j_2)} \ldots\ldots$$

$$(-1)^{m_r(j_{r-1} + i_0)} \} \times$$

$$\{(-1)^{m_{r-1}(i_0 + i_1)} . (-1)^{m_{r-2}(i_1 + i_2)} \ldots\ldots\ldots$$

$$(-1)^{m_0 \, i_{r-1}} \}. \qquad (6.2.12)$$

Writing down the binary representation of m (refer to equation (6.2.10)),

$$(m_{2r-1}, \ldots, m_r, m_{r-1}, \ldots, m_0) =$$

$$(t_{r-1}, t_{r-2}, \ldots, t_0, u_{r-1}, u_{r-2}, \ldots, u_0). \quad (6.2.13)$$

Replacing the m's in equation (6.2.12) by t's and u's by using equation (6.2.13),

$$h_N^{m,p} = \{(-1)^{t_{r-1}(j_0 + j_1)} . (-1)^{t_{r-2}(j_1 + j_2)} \ldots\ldots, (-1)^{t_0(j_{r-1} + i_0)}\} \times \{(-1)^{u_{r-1}(i_0 + i_1)} .. (-1)^{u_{r-2}(i_1 + i_2)} . (-1)^{u_0 i_{r-1}}\}$$

$$= \{\prod_{\alpha=0}^{r-1} (-1)^{t_{r-1-\alpha}(j_\alpha + j_{\alpha+1})}\} \times \{\prod_{\beta=0}^{r-1} (-1)^{u_{r-1-\beta}(i_\beta + i_{\beta+1})}\} (-1)^{t_0 i_0}$$

Using equation (6.2.7), we may then write

$$h_N^{m,p} = (h_n^{t,j} . h_n^{u,i}) (-1)^{t_0 i_0} \quad (6.2.14)$$

Substituting for $h_N^{m,p}$ in equation (6.2.8),

$$S_m^{(1)} = \sum_{p=0}^{N-1} h_N^{m,p} s_p^{(1)} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{u,i} s_{i,j}^{(2)} h_n^{t,j} (-1)^{t_0 i_0}$$

(6.2.15)

Now, two separate cases arise depending upon whether t is even or odd.

t is even: Since t is even, $t_0 = 0$ so that for all such m's for which t is even, equation (6.2.15) may be written as

$$S_m^{(1)} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{u,i} \, s_{i,j}^{(2)} \, h_n^{t,j} = S_{u,t}^{(2)} . \qquad (6.2.16)$$

Thus, when m with a (lexicographic) representation (t,u) is such that t is even,

$$S_{(t,u)}^{(1)} = S_m^{(1)} = S_{u,t}^{(2)} . \qquad (6.2.17)$$

t is odd: Since t is odd, $t_0 = 1$. Therefore equation (6.2.15) may be written as

$$S_m^{(1)} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{u,i} \, s_{i,j}^{(2)} \, h_n^{t,j} (-1)^{i_0}$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{i,u} \, s_{i,j}^{(2)} \, h_n^{t,j} (-1)^{i_0} .$$

Since i is even or odd depending upon whether i_0 is zero or 1,

$$S_m^{(1)} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{i,u} \, s_{i,j}^{(2)} \, h_n^{t,j} (-1)^{i}$$

$$= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{i,u} \, s_{i,j}^{(2)} \, h_n^{t,j} \, h_n^{i,(n-1)} .$$

In writing the last step of the above equation, use is made of the fact that the (n-1) column in the sequency ordered Hadamard matrix H_n, has +1 in even rows and -1 in odd rows. So,

$$S_m^{(1)} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} h_n^{i,u}\, h_n^{i,n-1}\, s_{i,j}^{(2)}\, h_n^{t,j} \,.$$

But $h_n^{i,u} \cdot h_n^{i,n-1} = h_n^{i,u \oplus (n-1)}$ (in view of equation A.24, Appendix A) where, $\oplus$ denotes pointwise binary addition.
Since $u \varepsilon Z_n$, we have

$$u \oplus (n-1) = (n-1) - u \,.$$

Hence, for t odd, we have

$$S_m^{(1)} = S_{(t,u)}^{(1)} = S_{(n-1)-u,t}^{(2)} \,. \tag{6.2.18}$$

Equations (6.2.17) and (6.2.18) which hold respectively for the cases t even and t odd, imply that $S^{(1)}$, the sequency ordered transfer characteristics vector of the equivalent 1-D dyadic P-I system (obtained by using the lexicographic index mapping given by equation (6.2.3)), is formed by reading off the entries of the specified 2-D transfer characteristics matrix $S^{(2)}$ in the manner indicated by the arrow heads inside this matrix.

$$\begin{bmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,n-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,n-1} \\ \vdots & \vdots & & \vdots \\ s_{n-1,0} & s_{n-1,1} & \cdots & s_{n-1,n-1} \end{bmatrix}$$

With its sequency ordered transfer characteristics obtained in this manner, the equivalent 1-D dyadic P-I system may now be implemented using a suitable approximation technique. We now give an example to illustrate the implementation of 2-D dyadic P-I filter in terms of its equivalent 1-D system.

Example 6.2.1: A 2-D dyadic P-I filter with $n = 32$, having ideal circularly symmetric low pass amplitude characteristics with a cutoff sequency of 15, is to be implemented. Amplitude response is 1 in pass band and zero in stop band.

This 2-D dyadic P-I filter is implemented in terms of its equivalent 1-D dyadic P-I system obtained by using the index mapping f given by equation (6.2.3). First, the sequency ordered transfer characteristics vector for this equivalent 1-D system is obtained using the result obtained in section 6.2.3. The equivalent 1-D system is then implemented using least-squares approximation technique [1]. For the purpose of this approximation, out of a total of 1024 entries, only

the first 256 entries of the unit sample response of the equivalent 1-D filter are considered. The implementation of the equivalent 1-D is carried out by dyadically convolving this approximate unit response vector with the 1-D equivalent (obtained through the use of index mapping f) of the 2-D finite discrete signal which was to be filtered. The 2-D version of the output signal so obtained, is the desired filtered output of the given 2-D P-I system. The realized transfer characteristics of the 2-D filter are shown in Fig. 6.4.

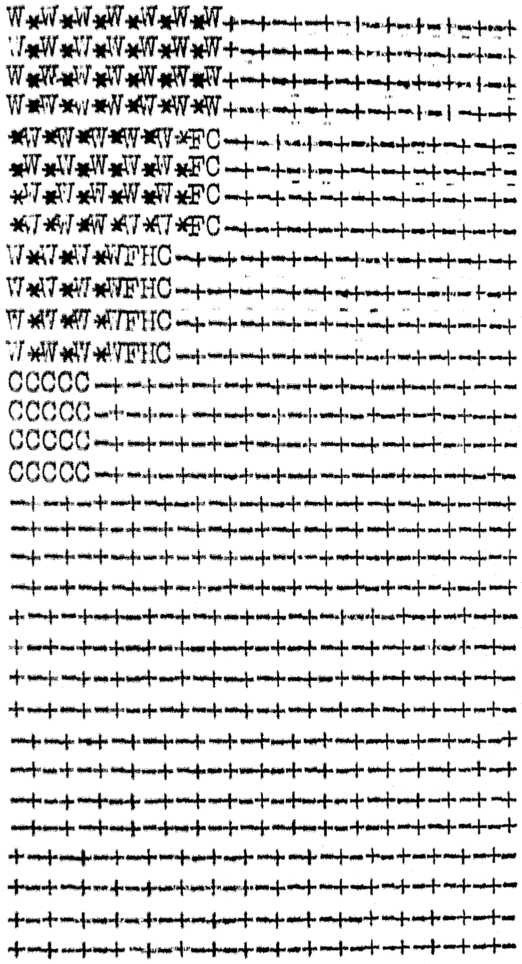


Fig. 6.4: Realized Amplitude Characteristics of the 2-D Dyadic P-I Filter in Example 6.2.1.

*	1.13	C	0.59
W	1.00	I	0.39
Z	0.99	+	0.09
B	0.89	-	-0.04
E	0.79		

CHAPTER 7

P-I SYSTEMS ON FINITE FIELDS AND RINGS

Our study has so far been concerned with P-I systems on vector spaces defined over the complex number field. In this chapter, we propose to study (i) P-I systems on vector spaces defined over finite fields and (ii) P-I systems on modules defined over ~~rings~~ integers of residue class ~~integers~~ rings. For convenience, we shall henceforth refer to these systems respectively as (i) P-I systems on finite fields, and (ii) P-I systems on rings. The input and output signals for P-I systems on finite fields are finite sequences with entries drawn from a finite field, while those for P-I systems on rings are finite sequences with entries drawn from a ring of residue class integers. The sample domain behaviour of these two new categories of P-I systems is dealt with briefly, covering only those aspects in which they differ from 1-D P-I systems having real-field inputs. The main concern here,

is to study these systems in the transform domain. It is shown here that just like the 1-D P-I systems with real-field inputs, these two categories of P-I systems also define finite discrete transforms. The transforms defined by cyclic class P-I systems on finite fields correspond to the 'Fourier transform in finite fields' [15], and the transforms defined by cyclic class P-I systems on rings will, by an appropriate choice of the modulus of the ring, lead to the various number-theoretic transforms [16, 17] that have been proposed in the last few years for efficient and error-free computation of convolutions

To begin with, in section 7.1 we deal with the minor modifications that are needed in the expressions for convolutions necessitated by the finite nature of the underlying finite field or ring. In the next four sections, P-I systems on finite fields are studied in detail. The ~~last~~ previous section, i.e., section 7.6 is devoted to a study of P-I systems on rings.

7.1 Convolutions in Finite Fields and Rings

It is known that a cyclic P-I system in the complex number field performs a cyclic convolution described by

$$y_k = \sum_{l=0}^{n-1} s_l \cdot x_{k \ominus l} \quad ; \quad k \in Z_n \, , \tag{7.1.1}$$

where $\ominus$ denotes subtraction modulo n. The symbols s, x, and y respectively denote the unit sample response, the input and the output sequences. When we consider cyclic P-I systems on a finite field of characteristic p (see definition 7.2.3) where p is a prime number, the entries of the sequences s, x and y in equation 7.1.1 are numbers of the field of integers modulo p. In the case of cyclic P-I systems on a ring of integers modulo p, where p is any integer, the entries of these sequences in equation 7.1.1, are from the ring of residue class integers modulo p. Hence, the cyclic convolution corresponding to both these cases - cyclic P-I systems on a finite fields of characteristic p, and on the ring of residue class integers modulo p, takes the form

$$y_k \equiv \left(\sum_{l=0}^{n-1} s_l \cdot x_{k \ominus l}\right) \bmod p$$

$$\equiv \left(\sum_{l=0}^{n-1} s_{k \ominus l}\, x_l\right) \bmod p \quad ; \quad k \varepsilon Z_n \; , \qquad (7.1.2)$$

where p is to be interpreted as the characteristic of the underlying finite field in the case of P-I systems on finite fields, and as the modulus of the underlying ring of residue class integers in the case of P-I systems on rings. Further, the symbol '$\equiv$' denotes congruence.

However, for a cyclic P-I system with a given integer sequence s as its unit sample response, if it is known that the input integer sequence x is bounded by the value $|x|_{max}$, then the congruence 7.1.2 is essentially an equality

$$y_k = \sum_{l=0}^{n-1} s_l \, x_{k \ominus l} \quad ; \quad k \varepsilon Z_n \, , \qquad (7.1.3)$$

provided, the value of p is suitably chosen so that

$$p > |x|_{max} \sum_{l=0}^{n-1} |s_l| \, . \qquad (7.1.4)$$

In the above inequality, p has to be a prime number when the P-I system is on a finite field and it may be any suitable integer when the system is on a ring of residue class integers.

In general, a P-I system on a finite field or on a ring of residue class integers, defined relative to a transitive abelian group G of order n, denotes a convolution operation given by equation(7.1.2) but with the understanding that the symbol $\ominus$ now denotes pointwise subtraction operation in the mixed-radix number system with the mixed-radices given by the invariants of the group G.

7.2 Finite Fields and the Problem of Identifying An Appropriate Extension Field

In our study of P-I systems on finite fields in this and the next three sections, certain standard results from the theory of finite fields will be made use of quite frequently. Hence, we begin this section by listing a few of the useful definitions and theorems pertaining to this theory.

Definition 7.2.1: The order of a field is equal to the number of elements in the field; if the order is finite, we call the field a finite field.

Theorem 7.2.1: Integers modulo p, where p is a prime, form a finite field of order p. For example, the set of integers modulo 7, i.e., $\{0,1,2,3,4,5,6\}$ forms a finite field of order 7.

Theorem 7.2.2: If p is a prime and m is any positive integer, then there exists a finite field of order p^m.

As an example, a finite field of order $2^2 = 4$ is formed by the elements $0,1,\alpha,\alpha^2$, where α is defined by the relation: $1 + \alpha = \alpha^2$. In general, if $f(x)$ is an irreducible polynomial of degree m with its coefficients in the field of integers mod p where p is a prime, then the residue classes mod $f(x)$ form a finite field of order p^m.

Definition 7.2.2: Let α be a non-zero element of a finite field. Then the least positive integer e for which $\alpha^e = 1$ is called the order of the element α. For example, in $GF(2^2) = \{0, 1, \alpha, \alpha^2\}$ considered in the previous example, the element α has an order 3 since $\alpha^3 = \alpha.\alpha^2 = \alpha(1 + \alpha) = 1$. The element α^2 also has the same order.

Theorem 7.2.3: A finite field of order q must contain at least one element which is primitive, i.e., one whose order is (q-1) and whose powers include all the non-zero field elements.

In the finite field of order 5, viz., $\{0, 1, 2, 3, 4\}$, formed by integers modulo the prime 5, the elements 2 and 3 are primitive elements and have an order 4 since 4 is the least positive integer satisfying $2^4 \equiv 1 \bmod 5$ and $3^4 \equiv 1 \bmod 5$. Further, $2^0 \equiv 1 \bmod 5$, $2^1 \equiv 2 \bmod 5$, $2^2 \equiv 4 \bmod 5$, $2^3 \equiv 3 \bmod 5$. Also, $3^0 \equiv 1 \bmod 5$, $3^1 \equiv 3 \bmod 5$, $3^2 \equiv 4 \bmod 5$, and $3^3 \equiv 2 \bmod 5$.

Definition 7.2.3: The least positive integer c, for which $ca = 0$ for every a of the field, is called the characteristic of the field.

In the field of residue class integers mod p where p is a prime, the characteristic is p.

Theorem 7.2.4: In a field of characteristic p, the field integers form a subfield of order p isomorphic to the field of integers modulo p.

Consider for example, the field $GF(2^2) = \{0, 1, \alpha, \alpha^2\}$. The field integers 0 and 1 form a subfield of GF(2) and $\{0,1\}$ is the field formed by the residue class integers modulo 2.

<u>Theorem 7.2.5</u>: In a finite field of order q, the order of every element must divide (q-1). Take for example $GF(2^4)$. It has an order q = 16, i.e., it has 16 elements. The characteristic being 2, the field integers are 0 and 1. If α be a primitive element of this field, then all the non-zero field elements must be generated by successive powers of α, viz., $\alpha^0, \ldots, \alpha^{14}$. The following table gives the orders of the various field elements. In this table, α is a root of the irreducible polynomial $x^4 + x + 1$.

Table 7.1: <u>$GF(2^4)$ Field Elements and their Orders</u>

S.No.	Field Element	Binary Representation	Order	S.No.	Field Element	Binary Representation	Order
1	0	0 0 0 0	-	6	α^4	0 0 1 1	15
2	1	0 0 0 1	-	7	α^5	0 1 1 0	3
3	α	0 0 1 0	15	8	α^6	1 1 0 0	5
4	α^2	0 1 0 0	15	9	α^7	1 0 1 1	15
5	α^3	1 0 0 0	5	10	α^8	0 1 0 1	15
				11	α^9	1 0 1 0	5

Table 7.1: (continued)

S.No.	Field Element	Binary Representation	Order
12	α^{10}	0 1 1 1	3
13	α^{11}	1 1 1 0	15
14	α^{12}	1 1 1 1	5
15	α^{13}	1 1 0 1	15
16	α^{14}	1 0 0 1	15

7.2.1 Identifying the Appropriate Extension Field

An element α in a finite field F, which is such that $\alpha^n = 1$, is called an n-th root of unity in F. If such an element α has an order n in F, it is called a primitive n-th root of unity in F. It will be seen in the next section i.e., section 7.3 that the n-th roots of unity in F play a central role in the development of the theory of P-I systems on F. In this connection, it is useful to recall (see remark 2.6.1) that while considering the characterization of 2-D P-I systems in terms of their eigenvectors and eigenvalues, we had moved over from the field of real numbers to its extension field, the complex number field, in view of the fact that the complex number field is algebraically closed while the real number field is not. In the complex number field, an n-th root of unity always exists for any given positive integer n, and

it is given by $\exp(\sqrt{-1}\,\frac{2\pi}{n})$. Similar situations necessitating the use of an extension field arise, in the study of many types of systems [42,43]. When we consider P-I systems of dimension n on a finite field $F = GF(p)$, where p is a specified prime number, we may come across a similar situation. For a given n, n-th roots of unity may or may not exist in F. In order to derive expressions for the eigenvectors and eigenvalues of P-I systems on finite fields, it may therefore become necessary to move over to an appropriate extension field, say $GF(p^m)$, which contains all the n-th roots of unity. In view of this, we shall first examine the question of existence of n-th roots of unity in F and the problem of identifying an appropriate extension field in case F does not have n-th roots of unity for a given n.

Consider a ground field GF(p) where, p is a given prime, and its m-th order algebraic extension viz., $F = GF(p^m)$, where m is a positive integer. F has p^m-1 non-zero elements which are all distinct, and by theorem 7.2.3, are powers of a primitive element say α, whose order is p^m-1. If γ be an n-th root of unity where n is some specified positive integer, then by theorem 7.2.5, $\gamma \varepsilon F$ iff n divides p^m-1. Hence we have,

<u>Theorem 7.2.6</u>: Let n be a positive integer. Then an n-th root of unity exists in $F = GF(p^m)$ iff n divides p^m-1, i.e., iff $p^m \equiv 1 \mod n$.

Theorem 7.2.7: If an n-th root of unity γ is in F, then the elements γ^i, $i \in Z_n$ are all in F, and they are all distinct.

Proof: Let α be a primitive element of F. Then, by theorem 7.2.3,

$$F = GF(p^m) = \{0, \alpha^1, \alpha^2, \ldots, \alpha^{p^m-1} = 1\}$$

and, all these p^m elements are distinct.

Now, let γ be a primitive n-th root of unity in F and let

$$\gamma = \alpha^k$$

where, k is a positive integer given by (refer to theorem 7.2.5)

$$k = \frac{p^m-1}{n}$$

Now, consider the following set of n elements; ~~viz., $\{\gamma^i\}$, $i\in Z_n$~~.

$$\{\gamma^i\} = \{1, \alpha^k, \alpha^{2k}, \ldots, \alpha^{(n-1)k}\}; \quad i \in Z_n. \quad (7.2.1)$$

The n elements in the above set thus correspond to distinct integer powers of α, a primitive element of F, with the index always less than (p^m-1). Hence, by theorem 7.2.3, they are all distinct elements of F. Now,

Theorem 7.2.8: Let n be a given positive integer. If m is the least positive integer such that n divides (p^m-1), then

the set $\{1, \alpha^k, \ldots, \alpha^{(n-1)k}\}$ includes all the n-th roots of unity in $F = GF(p^m)$, where α is a primitive element of the finite field F, and k is a positive integer given by $(p^m-1)/n$.

Proof: $k = \frac{p^m-1}{n}$

Therefore, $(\alpha^{ik})^n = \alpha^{i(p^m-1)} = (\alpha^{p^m-1})^i = 1^i = 1$ for every $i \varepsilon Z_n$,

i.e., $(\alpha^{ik})^n = 1$ for every $i \varepsilon Z_n$ (7.2.2)

But since α is a primitive element of F, α^{ik}, $i \varepsilon Z_n$ are all distinct elements of $F = GF(p^m)$. Thus, in view of equation (7.2.2), they are all distinct n-th roots of unity in $GF(p^m)$.

To show that all the n-th roots of unity are included in the above set, let β be an n-th root of unity in $GF(p^m)$ but not included in the above set. Sine $\beta \varepsilon GF(p^m)$, from theorem 7.2.3 we know that it must be some power of the primitive element α, so let $\beta = \alpha^l$. Since β is an n-th root of unity,

$$\beta^n = \alpha^{ln} = 1.$$

But $\alpha^{nk} = \alpha^{n(\frac{p^m-1}{n})} = 1$.

Therefore, $\alpha^{ln} = \alpha^{nk} = 1$.

Therefore, l must be a multiple of k.

This implies that β is in the set $\{\alpha^{ik}\}$, $i\varepsilon Z_n$. Thus, if n divides p^m-1 , $GF(p^m)$ contains n distinct n-th roots of unity and equation 7.2.1 enables us to locate them.

These results can be immediately applied to the problem of identifying an appropriate extension field for a given P-I system of dimension n. Thus, as we shall see in detail in the subsequent sections, if we are given a cyclic P-I system of dimension n on a vector space defined over the finite field GF(p), we first check whether n divides (p-1). If it does, all the elements of the eigenvectors of the system lie in the field GF(p). If n does not divide (p-1), we extend the given field GF(p) to $GF(p^m)$ such that n divides p^m-1 where m is the least positive integer satisfying this condition. Then it follows from the above results that $GF(p^m)$ has in it all the n distinct n-th roots of unity. Thus, $GF(p^m)$ is the extension field we seek.

Remark 7.2.1: If the characteristic p (a prime number) equals 2 and n is given to be even, or in general, if n is any multiple of the characteristic p, then there does not exist an m for which n divides p^m-1.

Remark 7.2.2: In view of the foregoing discussion, in our subsequent study of the theory of cyclic P-I systems, we shall assume that the cyclic P-I system acts on a vector space

defined over $GF(p^m)$ - an appropriately chosen extension field.

We will now consider a few examples that illustrate the ideas developed in this section.

Example 7.2.1: Consider a cyclic P-I system of order 3 on GF(2). Assume that the system matrix is given by

$$T = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Since m = 2 is the smallest positive integer, such that $2^m \equiv 1 \mod 3$, we first extend the given ground field GF(2) to $GF(2^2)$. Now, $GF(2^2) = \{0, 1, \alpha, \alpha^2\}$, where α is a root of the irreducible polynomial (irreducible in GF(2) but not in $GF(2^2)$); f(x) given by

$$f(x) = x^2 + x + 1$$

Thus, $GF(2^2)$ has 3 distinct 3rd roots of unity, these being $1, \alpha$ and α^2. From the system matrix we find that the characteristic polynomial of the matrix is

$$p(\lambda) = \lambda^3 + 1 = (\lambda + 1)(\lambda^2 + \lambda + 1) =$$
$$(\lambda + 1)(\lambda + \alpha)(\lambda + \alpha^2)$$

(Note: Since the underlying field has a characteristic equal to 2, the arithmetic to be used is modulo 2 arithmetic).

Therefore, the eigenvalues are $1, \alpha$ and α^2 and the corresponding eigenvectors are respectively

$$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \end{bmatrix}, \begin{bmatrix} 1 \\ \alpha^2 \\ \alpha \end{bmatrix}$$

Thus, all the entries of the eigenvectors are contained in the extension field $GF(2^2)$.

Example 7.2.2: Let $n = 5$, and $p = 2$. Since $m = 4$ is the smallest positive integer such that $p^m \equiv 1 \bmod n$, the extension field needed in this case is $GF(2^4)$. Let α be a primitive element of $GF(2^4)$,

$$GF(2^4) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}.$$

The 5 distinct fifth roots of unity in $GF(2^4)$ are therefore $1, \alpha^3, \alpha^6, \alpha^9$ and α^{12}.

7.3 Eigenvalues and Eigenvectors of Cyclic P-I Systems on Finite Fields

With the requisite background developed in the preceding sections, we are now in a position to proceed with the task of deriving specific expressions for the eigenvalues and eigenvectors of cyclic P-I systems on finite fields. After doing this, we shall use these expressions for deriving the transform pair defined by these cyclic P-I systems.

Let V be an n-dimensional vector space defined over a finite field $F = GF(p^m)$, where p is a prime and m is the least positive integer such that n divides (p^m-1). Let $\gamma \varepsilon F$ be an n-th root of unity in F. Then

$$\gamma^n = 1 . \tag{7.3.1}$$

Let P_k, $k \varepsilon Z_n$, be a member of G, a transitive abelian group of cyclic permutation matrices of order n. For a given $k \varepsilon Z_n$, P_k is an n x n matrix whose first column has a 1 in the k-th position and zeros elsewhere, and whose other columns are all cyclic permutations of the first column.

$$\begin{array}{r c}
 & \begin{array}{cccccccc} & & & & \text{(n-k)-th position} & & & \end{array} \\
P_k = & \left[\begin{array}{cccccccc}
0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \vdots \\
1 & 0 & \cdots & 0 & 0 & 0 & \cdots & \vdots \\
0 & 1 & \cdots & 0 & 0 & 0 & \cdots & \vdots \\
\vdots & 0 & \cdots & 0 & 0 & 0 & \cdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0
\end{array}\right] \\
\text{k-th position} \rightarrow \text{(row 6)} &
\end{array}$$

Note that a 1 appears in the (n-k)-th position in the first row. If we now define y_k as

$$y_k \stackrel{d}{=} \gamma^{n-k}, \tag{7.3.2}$$

then we find that

$$[P_k] \begin{bmatrix} 1 \\ \gamma \\ \gamma^2 \\ \vdots \\ \gamma^{n-1} \end{bmatrix} = y_k \begin{bmatrix} 1 \\ \gamma \\ \gamma^2 \\ \vdots \\ \gamma^{n-1} \end{bmatrix} \quad \text{for every } k\varepsilon Z_n . \tag{7.3.3}$$

Hence, $y_k \stackrel{d}{=} \gamma^{n-k} = \gamma^{-k}$ is an eigenvalue of P_k and the associated eigenvector is given by $[1\ \gamma\ \gamma^2 \ldots\ldots\ \gamma^{n-1}]^T$. From ~~remark~~ Theorem 7.2.8, we know that equation (7.3.1) has n distinct solutions in F given by

$$\gamma_\beta = \gamma_n^\beta \quad ; \quad \beta\varepsilon Z_n ; \tag{7.3.4}$$

where γ_n is a primitive n-th root of unity in F. Hence, γ has n distinct values and therefore, P_k has n distinct eigen-values given by

$$\sigma^{\beta,k} = \gamma_n^{-\beta k} \quad ; \quad \beta\varepsilon Z_n . \tag{7.3.5}$$

Thus, [30, p. 187] P_k has n independent eigenvectors and hence each P_k is individually diagonalizable. But then, we know that the P_k's, being members of an abelian group, commute pairwise.

i.e., $P_l \cdot P_m = P_m \cdot P_l$ for every $l,m\varepsilon Z_n$. (7.3.6)

Therefore, G is a commuting family of diagonalizable linear operators on the finite dimensional vector space V. From standard results in linear algebra it then follows [30 ,p.207] that there exists an ordered basis for V such that every operator in G is represented in that basis by a diagonal matrix. This basis is provided by the ordered set of n independent eigenvectors common to all P_k's, viz.,

$$(\varphi_n^0 , \varphi_n^1 , \varphi_n^2 , \ldots , \varphi_n^{n-1}),$$

where $$\varphi_n^\beta = (1\ \gamma_n^\beta\ \gamma_n^{2\beta} \ldots\ \gamma_n^{(n-1)\beta})^T \quad ; \beta\varepsilon Z_n , \qquad (7.3.7)$$

and γ_n is the primitive n-th root of unity in F given by

$$\gamma_n = \alpha^k \quad , \quad k = (\frac{p^m-1}{n}) \qquad (7.3.8)$$

and α is a primitive element of F.

The class of P-I systems on V relative to G, are known [1] to form a vector space of dimension n, where n is the degree and order of G, the transitive abelian group of cyclic permutation matrices. Members of this group, viz., P_k's, $k\varepsilon Z_n$, form a basis for this space. Since P_k's have been shown to have a common set of eigenvectors φ_n^β , $\beta\varepsilon Z_n$ that span the vector space V, it follows that the whole class of P-I

systems relative to G, has a common set of linearly independent eigenvectors, given by equation (7.3.7), that span the vector space V.

We now consider an example that illustrates the above ideas.

Example 7.3.1: Consider the class of cyclic P-I systems with 5-tuples drawn from a vector space defined over GF(2) as input vectors.

Thus, $p = 2$ and $n = 5$.

Since $m = 4$ is the least positive integer satisfying the condition $p^m \equiv 1 \bmod n$, the entries of the eigenvectors of this class of systems will be in $GF(2^4)$. Let the primitive 5-th root of unity in $GF(2^4)$ be γ. Then $\gamma = \alpha^3$ where α is a primitive element of $GF(2^4)$. Hence, the common set of eigenvectors of this class of P-I systems are

$$(1\ 1\ 1\ 1\ 1)^T,\ (1\ \gamma\ \gamma^2\ \gamma^3\ \gamma^4)^T,\ (1\ \gamma^2\ \gamma^4\ \gamma\ \gamma^3)^T,$$

$$(1\ \gamma^3\ \gamma\ \gamma^4\ \gamma^2)^T, \quad \text{and} \quad (1\ \gamma^4\ \gamma^3\ \gamma^2\ \gamma)^T$$

The modal matrix u for this class of P-I systems is therefore given by

$$u = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 \\ 1 & \gamma^2 & \gamma^4 & \gamma & \gamma^3 \\ 1 & \gamma^3 & \gamma & \gamma^4 & \gamma^2 \\ 1 & \gamma^4 & \gamma^3 & \gamma^2 & \gamma \end{bmatrix}$$

and $$u^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \gamma^4 & \gamma^3 & \gamma^2 & \gamma \\ 1 & \gamma^3 & \gamma & \gamma^4 & \gamma^2 \\ 1 & \gamma^2 & \gamma^4 & \gamma & \gamma^3 \\ 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 \end{bmatrix}.$$

If now P_k's, $k \varepsilon Z_n$ be members of a transitive abelian group of cyclic permutation matrices of degree and order 5, and $u^{-1} P_k u = \Lambda_k$, then we have,

$$\Lambda_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad \Lambda_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \gamma^4 & 0 & 0 & 0 \\ 0 & 0 & \gamma^3 & 0 & 0 \\ 0 & 0 & 0 & \gamma^2 & 0 \\ 0 & 0 & 0 & 0 & \gamma \end{bmatrix},$$

$$\Lambda_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \gamma^3 & 0 & 0 & 0 \\ 0 & 0 & \gamma & 0 & 0 \\ 0 & 0 & 0 & \gamma^4 & 0 \\ 0 & 0 & 0 & 0 & \gamma^2 \end{bmatrix}, \quad \Lambda_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \gamma^2 & 0 & 0 & 0 \\ 0 & 0 & \gamma^4 & 0 & 0 \\ 0 & 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & 0 & \gamma^3 \end{bmatrix},$$

and $\Lambda_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \gamma & 0 & 0 & 0 \\ 0 & 0 & \gamma^2 & 0 & 0 \\ 0 & 0 & 0 & \gamma^3 & 0 \\ 0 & 0 & 0 & 0 & \gamma^4 \end{bmatrix}$.

7.3.1 Transforms Defined by Cyclic P-I Systems on Finite Fields

The class of cyclic P-I systems on an n-dimensional vector space V over a finite field $F = GF(p^m)$, has been shown to have a common set of n linearly independent eigenvectors φ_n^β, $\beta \varepsilon Z_n$. Since these n vectors form a basis for V, if $x = (x_0\ x_1 \ldots x_{n-1})^T \varepsilon V$ be any arbitrary vector in V, then

$$x = X_0\ \varphi_n^0 + X_1\ \varphi_n^1 + \ldots + X_{n-1}\ \varphi_n^{n-1} = \sum_{i=0}^{n-1} X_i\ \varphi_n^i, \tag{7.3.9}$$

where X_i, $i\varepsilon Z_n$ are scalars belonging to F.

Therefore, the j-th component of x, viz., x_j is given by

$$x_j = \sum_{i=0}^{n-1} X_i\ \varphi_n^{i,j} = \sum_{i=0}^{n-1} X_i\ \gamma_n^{ij} \quad ; \quad j\varepsilon Z_n, \tag{7.3.10}$$

(refer to equation 8.3.7)

where $\varphi_n^{i,j} = \gamma_n^{ij}$ is the j-th component of the i-th eigenvector φ_n^i and γ_n is a primitive n-th root of unity in F.

Let the direct transform corresponding to equation 7.3.10 be of the form

$$X_i = K \sum_{j=0}^{n-1} x_j \, \gamma_n^{-ij} \quad ; \quad i \varepsilon Z_n \, , \tag{7.3.11}$$

where $K \varepsilon F$ is a normalizing scalar yet to be determined.

Substituting for X_i from equation (7.3.11) in equation (7.3.10), we have,

$$x_j = K \sum_{i=0}^{n-1} \gamma_n^{ij} \sum_{l=0}^{n-1} x_l \, \gamma_n^{-il} = K \sum_{l=0}^{n-1} x_l \sum_{i=0}^{n-1} \gamma_n^{i(j-l)} .$$

But we know that [15]

$$\sum_{i=0}^{n-1} \gamma_n^{iq} = \begin{cases} n & \text{if } q \equiv 0 \bmod n \\ 0 & \text{otherwise} \end{cases} .$$

Hence,

$$x_j = K \sum_{l=0}^{n-1} x_l \sum_{i=0}^{n-1} \gamma_n^{i(j-l)} = K x_j n \, . \tag{7.3.12}$$

Therefore, the normalizing constant K must be such that

$$Kn = 1 \, . \tag{7.3.13}$$

Since the field F is of characteristic p, all the summations used above are of mod p and hence, we may write equation (7.3.13) as

$$Kn \equiv 1 \bmod p \, . \tag{7.3.14}$$

Since we know that

$$p^m - 1 \equiv -1 \pmod{p},$$

it follows that $K = -M$ where M is such that

$$Mn = p^m - 1 \, .$$

Further, for convenience, we may transfer the normalizing scalar to the inverse transform. Hence, the direct transform may be written

$$X_i = \left(\sum_{j=0}^{n-1} x_j \, \gamma_n^{-ij}\right) \bmod p \quad ; \quad i \varepsilon Z_n \, , \qquad (7.3.15)$$

and the inverse transform may be written

$$x_j = \left(-M \sum_{i=0}^{n-1} X_i \, \gamma_n^{ij}\right) \bmod p \quad ; \quad j \varepsilon Z_n \, , \qquad (7.3.16)$$

where γ_n is the primitive n-th root of unity in F and M is an integer such that

$$Mn = p^m - 1 \, . \qquad (7.3.17)$$

Equations (7.3.16) and (7.3.17) define a transform pair. It may be observed that these exactly correspond to the 'Fourier transform in finite fields' proposed by Pollard [15]. Since cyclic P-I systems perform cyclic convolution and the Fourier transform has cyclic convolutional property, this is to be expected. But the P-I system approach used here has the

advantage that it leads in a natural way to a family of generalized transforms in finite fields. These transforms possess a generalized convolutional property so that the Fourier transform in finite fields derived in this section, becomes but a special case of this larger family of the generalized transforms. Utilizing the results of this section, we will be deriving these generalized transforms in the next section.

7.4 Generalized Transforms in Finite Fields

Let P_k, $k\varepsilon Z_n$ be a member of a transitive abelian group G of permutation matrices of degree and order n. Let m_α, $\alpha\varepsilon Z_r$ be the invariants of group G so that

$$n = \prod_{\alpha=0}^{r-1} m_\alpha \quad . \tag{7.4.1}$$

Then, G can be expressed as the direct product of r cyclic groups of orders m_α, $\alpha\varepsilon Z_r$. Hence, $P_k\varepsilon G$ may be written as

$$P_k = Q_{k_{r-1}} \otimes Q_{k_{r-2}} \otimes \cdots \otimes Q_{k_\alpha} \otimes \cdots \otimes Q_{k_0} \quad ; \; k\varepsilon Z_n \; , \tag{7.4.2}$$

where k_α, $\alpha\varepsilon Z_r$ are the mixed-radix digits in the mixed-radix representation of $k\varepsilon Z_n$ with respect to the mixed-radices m_α, $\alpha\varepsilon Z_r$ and Q_{k_α} is a cyclic permutation matrix of order m_α, $\alpha\varepsilon Z_r$. The symbol $\otimes$ represents Kronecker product

of matrices, the product matrix being written down using the familiar lexicographic ordering of indices.

Since n divides p^m-1 and each one of the m_α, $\alpha \varepsilon Z_r$ divides n (refer to equation(7.4.1)), the order of each one of the constituent cyclic matrices Q_{k_α}, viz., m_α divides p^m-1. Thus, our earlier results pertaining to cyclic matrices Q_{k_α}, $\alpha\varepsilon Z_r$, $k\varepsilon Z_n$. Hence, from equation (7.3.7), we may say that a cyclic permutation matrix such as Q_{k_α} has the following set of m_α linearly independent eigenvectors $\varphi^{\beta}_{m_\alpha}$, $\beta\varepsilon Z_{m_\alpha}$ and m_α distinct eigenvalues $\sigma^{\beta,k_\alpha}_{m_\alpha}$; β, $k_\alpha \varepsilon Z_{m_\alpha}$, where

$$\varphi^{\beta}_{m_\alpha} = (1 \; \gamma^{\beta}_{m_\alpha} \; \gamma^{2\beta}_{m_\alpha} \; \ldots\ldots \; \gamma^{k_\alpha\beta}_{m_\alpha} \; \ldots\ldots \; \gamma^{(m_\alpha-1)\beta}_{m_\alpha})^T$$

$$; \quad \beta,\ k_\alpha \varepsilon Z_{m_\alpha},\ \alpha\varepsilon Z_r \ ; \qquad (7.4.3)$$

and $$\sigma^{\beta,k_\alpha}_{m_\alpha} = \gamma^{-\beta k_\alpha}_{m_\alpha} \quad ; \quad \beta,\ k_\alpha\varepsilon Z_{m_\alpha} \text{ and } \alpha\varepsilon Z_r . \qquad (7.4.4)$$

γ_{m_α} in the above equations, is the primitive m_α-th root of unity in F. Now, following the arguments of Siddiqi [1, also Appendix A.7], in view of equation (7.4.2), the modal matrix H_n of P_k, $k\varepsilon Z_n$ is the direct product of the modal matrices U_{m_α} of the constituent cyclic matrices Q_{k_α}, $\alpha\varepsilon Z_r$.

Hence, the j-th eigenvector of P_k, viz., h^j_n is the direct product of the j_{r-1}-th, j_{r-2}-th, ... , j_α-th, ...,

j_0-th eigenvectors of $Q_{k_{r-1}}, Q_{k_{r-2}}, \ldots, Q_{k_\alpha}, \ldots, Q_{k_0}$ respectively, where j_α, $\alpha\varepsilon Z_r$ are the mixed-radix digits in the expansion of j with respect to the mixed-radices m_α, $\alpha\varepsilon Z_r$. That is,

$$h_n^j = \varphi_{m_{r-1}}^{j_{r-1}} \otimes \ldots \otimes \varphi_{m_\alpha}^{j_\alpha} \otimes \ldots \otimes \varphi_{m_0}^{j_0}, \quad (7.4.5)$$

where from equation (7.4.3) we know that

$$\varphi_{m_\alpha}^{j_\alpha} = (1 \; \gamma_{m_\alpha}^{j_\alpha} \; \gamma_{m_\alpha}^{2j_\alpha} \ldots \gamma_{m_\alpha}^{\beta j_\alpha} \ldots \gamma_{m_\alpha}^{(m_\alpha-1)j_\alpha})^T$$

$$; \; j_\alpha, \beta\varepsilon Z_{m_\alpha}. \quad (7.4.6)$$

Then it follows that the i-th component of h_n^j viz., $h_n^{i,j}$ is given by

$$h_n^{i,j} = \gamma_{m_{r-1}}^{i_{r-1}j_{r-1}} \gamma_{m_{r-2}}^{i_{r-2}j_{r-2}} \ldots \gamma_{m_\alpha}^{i_\alpha j_\alpha} \ldots \gamma_{m_0}^{i_0 j_0}$$

$$= \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{i_\alpha j_\alpha}, \quad (7.4.7)$$

where i_α, $\alpha\varepsilon Z_r$ are the mixed-radix digits in the expansion of i with respect to the mixed-radices m_α, $\alpha\varepsilon Z_r$.

Again, in view of equation (7.4.2), $\sigma_n^{j,k}$, the j-th eigenvalue of P_k is equal to the product of the j_{r-1}-th, ..., j_α-th, ... and j_0-th eigenvalues of the constituent cyclic

matrices viz., $Q_{k_{r-1}}$, $Q_{k_{r-2}}$, ..., Q_{k_α}, ... , ..., Q_{k_0} respectively. Hence,

$$\sigma_n^{j,k} = \sigma_{m_{r-1}}^{j_{r-1},k_{r-1}} \cdots\cdots \sigma_{m_\alpha}^{j_\alpha,k_\alpha} \cdots\cdots \sigma_{m_0}^{j_0,k_0} .$$

Using equation (7.4.4), we may rewrite the above as

$$\sigma_n^{j,k} = \gamma_{m_{r-1}}^{-j_{r-1}k_{r-1}} \cdots\cdots \gamma_{m_0}^{-j_0k_0} = \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{-j_\alpha k_\alpha} = \bar{h}_n^{j,k} , \tag{7.4.8}$$

where, $\bar{h}_n^{j,k}$ is the multiplicative inverse of $h_n^{j,k}$ in F.

We now observe that each one of the modal matrices U_{m_α}, $\alpha\varepsilon Z_r$ pertaining to the constituent cyclic matrices Q_{k_α}, is a symmetric matrix similar in nature to the generalized Hadamard matrices of Butson[35] of order m_α and that its entries are m_α-th roots of unity in F. Since the modal matrix H_n of each P_k, $k\varepsilon Z_n$, is the direct product of the modal matrices U_{m_α}, $\alpha\varepsilon Z_r$, H_n is also a generalized Hadamard matrix of order $n = \prod_{\alpha=0}^{r-1} m_\alpha$ and its entries are η-th roots of unity in F, where η is the least common multiple of m_0, m_1, m_2, ... , m_{r-1}. The i,j-th element of H_n is $h_n^{i,j}$ which is given by equation (7.4.7) from which it is seen that

$$h_n^{i,0} = h_n^{0,j} = 1 \quad ; \quad i,\ j\varepsilon Z_n , \tag{7.4.9}$$

and $\quad h_n^{i,j} = h_n^{j,i}$. (7.4.10)

Therefore, the generalized Hadamard matrix H_n is symmetric and is in standard form. It then follows from the properties of generalized Hadamard matrices [35] that

$$\sum_{j=0}^{n-1} h_n^{i,j} = \sum_{j=0}^{n-1} \bar{h}_n^{i,j} = n\delta_{0,i} \quad ; \quad i \varepsilon Z_n \qquad (7.4.11)$$

$$\sum_{i=0}^{n-1} h_n^{i,j} = \sum_{i=0}^{n-1} \bar{h}_n^{i,j} = n\delta_{0,j} \quad ; \quad j \varepsilon Z_n ,$$

and

$$\sum_{i=0}^{n-1} h_n^{i,k} \; \bar{h}_n^{i,j} = n\delta_{k,j} \quad ; \quad k, j \varepsilon Z_n \qquad (7.4.12)$$

$$\sum_{k=0}^{n-1} h_n^{i,k} \; \bar{h}_n^{j,k} = n\delta_{i,j} . \quad ; \quad i, j \varepsilon Z_n$$

Further, from equation (7.4.7) it follows that

$$h_n^{i,j} \, h_n^{i,k} = h_n^{i,j \oplus k} , \qquad (7.4.13)$$

where (+) denotes pointwise addition operation in the mixed-radix number system with mixed-radices $m_{r-1}, m_{r-2}, \ldots , m_0$.

Remark 7.4.1: The n x n matrix whose i,j-th element is $\bar{h}_n^{i,j}$, the multiplicative inverse of $h_n^{i,j}$ in F, will be denoted by H_n^*.

Then,

$$H_n \cdot H_n^* = n\, I_n, \tag{7.4.14}$$

where, I_n is an identity matrix of order n. Hence, it follows that

$$H_n^{-1} = \frac{1}{n} H_n^* = -M\, H_n^*, \tag{7.4.15}$$

where, the integer M is such that

$$Mn = p^m - 1. \tag{7.4.16}$$

In view of the fact that the class of P-I systems relative to G constitutes a vector space of dimension n for which the P_k's form a basis, the eigenvectors h_n^j , $j \varepsilon Z_n$ of the P_k's $k \varepsilon Z_n$, constitute the common set of eigenvectors for any P-I system defined relative to G. Further, these eigenvectors, being linearly independent, constitute a basis for V, the signal space on which the class of P-I systems operates. Therefore, if $x \varepsilon V$ is any arbitrary signal given by

$$x = (x_0\ x_1\ x_2\ \ldots.\ x_{n-1})^T \varepsilon V, \tag{7.4.17}$$

then, we may write

$$x = \left(\sum_{j=0}^{n-1} X_j\, h_n^j\right) \bmod p, \tag{7.4.18}$$

where, X_j is the j-th component of the vector $X = (X_0\ X_1\ \dots\ X_{n-1})^T$. With the understanding that the arithmetic involved is of mod p, we may write equation (7.4.18) as

$$x = H_n X . \tag{7.4.19}$$

From equations (7.4.15) and (7.4.19) we may write

$$X = H_n^{-1} x = - M H_n^* x . \tag{7.4.20}$$

After transfering the normalizing constant -M from equation (7.4.20) to equation (7.4.19), we may rewrite these equations alternatively as

$$X_k = \left(\sum_{j=0}^{n-1} \bar{h}_n^{k,j} x_j\right) \bmod p \quad ; \quad k \varepsilon Z_n , \tag{7.4.21}$$

and $$x_j = \left(-M \sum_{k=0}^{n-1} h_n^{k,j} X_k\right) \bmod p \quad ; \quad j \varepsilon Z_n , \tag{7.4.22}$$

where, $$h_n^{k,j} = \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{j_\alpha k_\alpha} \quad ; \quad j,\ k \varepsilon Z_n , \tag{7.4.22}$$

γ_{m_α} is the primitive m_α-th root of unity in F,

m_α, $\alpha \varepsilon Z_r$ are the invariants of the group G relative to which the pertinent class of P-I systems is defined,

j_α and k_α are the mixed-radix digits in the expansion of j and k respectively with respect to mixed-radices m_α, $\alpha \varepsilon Z_r$,

$\bar{h}_n^{k,j}$ is the (k,j)-th element of H_n^* and equals the multiplicative inverse in F of $h_n^{k,j}$, and

M is an integer in F such that

$Mn = p^m - 1$.

<u>Remark 7.4.2</u>: ~~The~~ Equations (7.4.21) and (7.4.22) define a transform pair which will be called the generalized finite discrete transform (FDT) pair in the finite field $GF(p^m)$. X will be called the FDT of x, and x, the inverse FDT of X.

It may be observed that for the particular case wherein G is a cyclic group of order n, the invariant is n so that $h_n^{j,k} = \gamma_n^{jk}$. Thus, in this case, ~~the~~ equations (7.4.21) and (7.4.22) reduce to those of the Fourier transform in finite fields given by equations (7.3.15) and (7.3.16).

7.5 Generalized Convolution Theorem for P-I Systems on Finite Fields

The generalized convolutional relationship between the input and output vectors of a P-I system on $GF(p^m)$ was given in section 1. This, together with the generalized FDT derived in the previous section, leads us to the generalized

convolutional theorem, according to which, the generalized FDT of the convolution of two signals is equal to the pointwise product mod p, of the corresponding elements of the generalized FDT's of the individual signals. Formally, let the vectors x,s and y be respectively the input, unit sample response and the output pertaining to a P-I system on $GF(p^m)$. Also, let X, S and Y be the generalized FDT's of x, s and y respectively. Then

$$Y_k = \left(\sum_{i=0}^{n-1} \bar{h}_n^{k,i}\, y_i\right) \bmod p \quad ; \quad k \varepsilon Z_n . \tag{7.5.1}$$

But, from equation 7.1.2, we have,

$$y_i = \left(\sum_{j=0}^{n-1} s_{i \ominus j}\, x_j\right) \bmod p \quad ; \quad i \varepsilon Z_n , \tag{7.5.2}$$

where $\ominus$ denotes pointwise subtraction in the mixed-radix number system with mixed-radices that are invariants of the pertinent transitive abelian group G relative to which the P-I system is defined. Therefore, substituting equation (7.5.2) in (7.5.1) we have,

$$Y_k = \left(\sum_{i=0}^{n-1} \bar{h}_n^{k,i} \left(\sum_{j=0}^{n-1} s_{i \ominus j} x_j\right) \bmod p\right) \bmod p$$

$$= (\sum_{j=0}^{n-1} x_j (\sum_{i=0}^{n-1} \bar{h}_n^{k,i} s_{i \ominus j}) \bmod p) \bmod p .$$

Now, substituting $l = i - j$ in the above, we have

$$Y_k = (\sum_{j=0}^{n-1} x_j (\sum_{l=0}^{n-1} \bar{h}_n^{k,l \oplus j} s_l) \bmod p) \bmod p .$$

But (refer to equation (7.4.13)) we know that

$$\bar{h}_n^{k,l \oplus j} = \bar{h}_n^{k,l} \; h_n^{k,j} .$$

Therefore,

$$Y_k = (((\sum_{j=0}^{n-1} \bar{h}_n^{k,j} x_j) \bmod p) \times$$

$$((\sum_{l=0}^{n-1} \bar{h}_n^{k,l} s_l) \bmod p)) \bmod p$$

$$= (X_k \cdot S_k) \bmod p .$$

Therefore, (7.5.3)

$$Y_k = (X_k \cdot S_k) \bmod p .$$

Thus we have established the generalized convolution theorem for P-I systems on finite fields.

7.6 P-I Systems in Rings of Residue Class Integers

In this section, we study the theory of P-I systems on modules defined over a ring Z_P of residue class integers modulo P, where P is a positive integer. These P-I systems have as their input and output signals, sequences of some arbitrary length n, whose entries are drawn from the elements of Z_P. The sample domain description of these systems is structurally the same as that of P-I systems over vector spaces; the minor modifications that are needed in the expressions for convolutions, necessitated by the nature of the underlying ring, have already been indicated in section 7.1. The main concern here is to develop the transform domain theory of this category of P-I systems. As a first step in the development of this theory, we consider the cyclic class P-I systems, and later we extend the results obtained for this class to general classes of P-I systems.

Consider a cyclic permutation matrix P_k belonging to G, a group of cyclic permutation matrices of degree and order n. That such a cyclic permutation matrix has powers of the n-th roots of unity as the entries in its eigenvectors, was shown in section 7.3 in the process of deriving expressions for the eigenvalues and eigenvectors of cyclic P-I systems on a finite field, F. For obtaining that result concerning the entries of eigenvectors of cyclic permutation matrices,

we made use of the property of a field not shared by a ring, only when the multiplicative inverse of an n-th root of unity in F was utilized. In this context it is to be noted that even though, every element of a ring need not have an inverse, an n-th root of unity, say γ, if it exists, then it does have an inverse, the inverse being γ^{n-1}. Hence we conclude the following:

Remark 7.6.1: The result of section 7.3 concerning the entries of the eigenvectors of cyclic permutation matrices can be applied to the ring Z_p also, provided an n-th root of unity exists in this ring.

Hence, to begin with, we shall first examine this question of the existence of n-th roots of unity in Z_p, and the methods to determine them. Later, using these n-th roots of unity, we will proceed with the task of deriving expressions for the eigenvalues and eigenvectors of cyclic P-I systems on a ring Z_p.

The use of the term 'eigenvector' in the context of modules perhaps requires clarification. Just as we talk of an eigenvector of a transformation on a vector space, by an eigenvector of a transformation t on a module M, we mean here a member $x \varepsilon M$ such that

$$tx = \lambda x ,$$

where λ is in the ring underlying M. The existence of either the eigenvalues or the eigenvectors is not in general guaranteed in this case. However, as we shall presently see, with a suitable choice of the dimensions of the modules and the P-I systems on them, we are assured of the existence of these eigenvalues and eigenvectors.

7.6.1 n-th Roots of Unity in Z_P

As mentioned earlier, we now examine the question of finding the n-th roots of unity in Z_P. We do this in three stages. First we consider the simple case when P is a prime number. Next we assume that P is some power of a prime number. Then, finally we consider the most general case when P is any arbitrary positive integer.

a. P is a prime number: When the modulus P of the ring Z_P is a prime number, say p, the residue class integers modulo P viz., $0,1,2,\ldots,(p-1)$, form a finite field F of order p. The method for determining the n-th roots of unity in this case, has already been discussed in detail in section 7.2. However, for the sake of completeness, we briefly summarize those results.

   The order of any element in F must divide $(p-1)$ since p is the order of the finite field F. An element $y \varepsilon F$ with an order of $(p-1)$ is called a primitive element of F and we know that every finite field will have a primitive element. Then the various powers of y generate all the non-zero elements of F so that

$F = \{0, y^1, y^2, \ldots, y^{p-1} = 1\}$. If $x \varepsilon F$ has an order n, then n divides (p-1). Since $x \varepsilon F$, let $x = y^{(p-1)/n}$. Then $x, x^2, x^3, \ldots, x^n$ will all be distinct elements of F and all these n elements are n-th roots of unity in F. The element x, which has an order n is known as the primitive n-th root of unity in F and successive powers of it generate all the n possible n-th roots of unity in F. Thus, if (p-1) is divisible by n, then there are n number of n-th roots of unity in the field F of residue class integers modulo p where p is a prime. If (p-1) is not divisible by n there will be no n-th roots of unity in F. Further, once we identify a primitive element of F, the method outlined herein can be used to determine all the n-th roots of unity in F.

Example 7.6.1: Consider the residue class integers modulo 7. These form a finite field F of order 7 given by $F = \{0,1,2,3,4,5,6\}$. The elements 3 and 5 belonging to F have an order of 6, i.e., 6 is the smallest positive integer such that

$$3^6 \equiv 1 \bmod 7,$$

and $$5^6 \equiv 1 \bmod 7.$$

Hence 3 and 5 are primitive elements of F. Considering 3 as the primitive element,

$$F = \{0, 3^1, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\}.$$

Therefore, if n = 3, a primitive 3rd root of unity in F is $3^{6/3} = 9 \equiv 2 \bmod 7$. Therefore, 2 is a primitive 3rd root of unity in F. Hence, the three 3rd roots of unity in F are 2^1, 2^2 and 2^3, i.e., 2, 4, and 1.

Note that even if we express all the non-zero elements of F as powers of the other primitive element, viz., 5, we will obtain the same set of 3rd roots of unity in F.

b. P Equals the power of a prime: Now, let us consider the ring Z_P, $P = p^e$, where p is a prime number and e is some positive integer. In Z_P the multiplicative order of any element is defined if and only if the element is relatively prime to p^e. The number of such elements in Z_P is given by Euler's phi function $\varphi(p^e) = p^{e-1}(p-1)$. The set of non-zero elements of Z_P that are relatively prime to p^e will henceforth be denoted by $P(p^e)$. Then it is known [45 ,p.32] that $P(p^e)$ forms a multiplicative cyclic group of order $\varphi(p^e)$. For p greater than 2, (it will be clear ~~from~~ in the sequel that this is but a trivial restriction), any element of P(p), i.e., the field of integers modulo p, which is greater than 1 can be a generator of this cyclic group. Let y be an element of this cyclic group $P(p^e)$ and let its order be n. Then n must divide the order of the cyclic group i.e. must divide $\varphi(p^e)$. Since $\varphi(p^e) = p^{(e-1)}(p-1)$ and p is a prime, it follows that n must either be equal to p^q, where q is an integer such that $0 < q < (e-1)$, or else it must divide (p-1). Now, if x be the generator of this cyclic group $P(p^e)$, $x^{\varphi(p^e)} \equiv 1 \bmod P$. Since $y \varepsilon P(p^e)$ is an n-th root of unity, $y = x^{\varphi(p^e)/n}$. Then the elements of the set $\{y^1, y^2, \ldots\ldots, y^n\}$ are distinct elements of $P(p^e)$ and form the set of n n-th roots of unity in Z_P. Thus, there are n possible n-th roots of unity in Z_P if n divides $\varphi(p^e)$; otherwise, there will not be any n-th root of unity in Z_P.

Further, the element y defined as above, is a primitive n-th root of unity in Z_p.

Remark 7.6.2: An element $y \varepsilon P(p^e)$ which has an order n is called primitive n-th root of unity in Z_{p^e}.

Example 7.6.2: Consider R, the ring of residue class integers modulo $9 = 3^2$.

$$R = \{0,1,2,3,4,5,6,7,8\}$$

$\varphi(3^2) = 3^1(3-1) = 6$. Thus, there are 6 integers in R that are relatively prime to 9. These are 1,2,4,5,7 and 8. These constitute a multiplicative cyclic group of order 6. As mentioned earlier, any integer greater than 1 which is an element of the field F of integers modulo 3, can be a generator of this group. In this case,

$$F = \{0,1,2\}.$$

Hence, the generator of the cyclic group is 2 in this case. Thus, we have,

$$\begin{aligned}
2 &\equiv 2 \bmod 9 \\
2^2 &\equiv 4 \bmod 9 \\
2^3 &\equiv 8 \bmod 9 \\
2^4 &\equiv 7 \bmod 9 \\
2^5 &\equiv 5 \bmod 9 \\
2^6 &\equiv 1 \bmod 9 .
\end{aligned}$$

If we now have n = 2, a primitive 2nd root of unity in R is given by $2^{6/2} = 8$. Then, $8^1 \equiv 8 \bmod 9$ and $8^2 \equiv 1 \bmod 9$, so that 1 and 8 are the two second roots of unity in R. If n = 3, a primitive third root of unity is given by $2^{6/3} \equiv 4 \bmod 9$. Then,

$4^1 \equiv 4 \bmod 9$, $4^2 \equiv 7$, and $4^3 \equiv 1 \bmod 9$ so that 1,4, and 7 constitute the three 3rd roots of unity in R.

c. P, the modulus is an arbitrary positive integer.

Let the unique prime power factorization of P yield,

$$P = \prod_{i=0}^{r-1} p_i^{e_i} = p_0^{e_0} \cdot p_1^{e_1} \cdots\cdots p_{r-1}^{e_{r-1}}, \qquad (7.6.1)$$

where p_i, $i\varepsilon Z_r$ are distinct primes and e_i, $i\varepsilon Z_r$ are positive integers.

We now define a ring R^* as the direct sum of the rings R_i, $i\varepsilon Z_r$ as follows:

$$R^* = (R_0, R_1, R_2, \dots, R_i, \dots, R_{r-1}), \qquad (7.6.2)$$

where each R_i, $i\varepsilon Z_r$, is the ring of residue class integers modulo $p_i^{e_i}$. Thus, in this ring R^*, an arbitrary element a will have a representation:

$$a = (a_0, a_1, a_2, \dots, a_i, \dots, a_{r-1});$$

$$a\varepsilon R^*, \ a_i \varepsilon R_i, \ i\varepsilon Z_r . \qquad (7.6.3)$$

If a and b be any two arbitrary elements in R^*, addition $\oplus$ and multiplication $\odot$ operations in the ring R^* are defined by

$$a \oplus b \stackrel{d}{=} (x_0, x_1, \dots, x_i, \dots, x_{r-1}), \qquad (7.6.4)$$

where $x_i \stackrel{d}{=} (a_i + b_i) \bmod p_i^{e_i}$,

and, $a \odot b \stackrel{d}{=} (y_0, y_1, \ldots, y_i, \ldots, y_{r-1},$

$$\text{where } y_i \stackrel{d}{=} (a_i \cdot b_i) \bmod p_i^{e_i}. \tag{7.6.5}$$

Since the number of elements in a constituent ring $R_i = p_i^{e_i}$, the total number of elements in the ring R^* is given by

$$\prod_{i=0}^{r-1} p_i^{e_i} = P .$$

There is an isomorphism between the ring R^* and the ring Z_P of residue class integers modulo P and the mapping between them is provided by the Chinese remainder theorem (CRT) [44]. If we let $m_i = p_i^{e_i}$, $i \varepsilon Z_r$ and consider an element $a \varepsilon R^*$ having a representation given by equation (7.6.3), then the element $b \varepsilon Z_P$ that corresponds to $a \varepsilon R^*$, is given by the CRT as

$$|b|_P = \left| \sum_{i=0}^{r-1} \hat{m}_i \left| a_i \left| \frac{1}{\hat{m}_i} \right| \right|_{m_i} \right|_P =$$

$$= \left| \sum_{i=0}^{r-1} \hat{m}_i \left| a_i \left| \frac{1}{\hat{m}_i} \right| _{m_i} \right| _{m_i} \right|_P , \tag{7.6.6}$$

where $\hat{m}_i = \frac{P}{m_i} = \frac{P}{p_i^{e_i}}$,

$$P = \prod_{i=0}^{r-1} m_i = \prod_{i=0}^{r-1} p_i^{e_i} ,$$

$\left| \frac{1}{\hat{m}_i} \right|_{m_i}$ = (multiplicative inverse of $\hat{m}_i$) mod m_i,

and $|q|_k$ stands for q mod k.

Remark 7.6.3: According to this direct sum representation of Z_p, the unity element of Z_p has a representation $1 = \langle 1, 1, \ldots, 1, \ldots, 1 \rangle$.

With this background we are now in a position to show that there exist n distinct n-th roots of unity in Z_p and also identify them.

Let $\alpha_i \varepsilon R_i$, $i \varepsilon Z_r$, be a primitive n-th root of unity in R_i. This means that n is the smallest positive integer such that $\alpha_i^n \equiv 1 \bmod p_i^{e_i}$. In section 7.6.1 it has already been shown that such an element α_i exists in R_i if and only if n divides $(p_i - 1)$ or $p_i^{(e_i-1)}$. Since p_i's are distinct primes, it follows that a primitive n-th root of unity exists in each one of the R_i's if and only if n divides each (p_i-1), $i = 0, 1, \ldots, (r-1)$. In other words, n must divide $((P_0-1), (p_1-1), (p_2-1), \ldots, (p_i-1), \ldots, (p_{r-1}-1))$, where (a,b) denotes the g.c.d. of a and b. This g.c.d then represents the largest value that n can possibly have, for a given modulus P. It may be mentioned here that Agarwal and Burrus [20] have given this condition, namely, that n must divide the g.c.d $((p_0-1), (p_1-1), \ldots, (p_i-1), \ldots, (p_{r-1}-1))$, as the single necessary and sufficient condition for n to be a possible number theoretic transform length in Z_p. Assuming that the given n divides the g.c.d. stated above, a primitive n-th root of unity γ_n in Z_p may then be represented by

$$\gamma_n = (\alpha_0, \alpha_1, \alpha_2, \dots , \alpha_i, \dots , \alpha_{r-1}), \qquad (7.6.7)$$

where, each $\alpha_i \varepsilon R_i$, $i \varepsilon Z_r$, is a primitive n-th root of unity in R_i. Then, since α_i^q, $q = 0, 1, \dots , (n-1)$ form distinct n-th roots of unity in R_i, $i \varepsilon Z_r$, and since the representation in equation (7.6.7) is unique, it follows that γ_n^q, $q = 0, 1, \dots , (n-1)$ form a set of n distinct n-th roots of unity in Z_p.

7.6.2 Eigenvalues and Eigenvectors

If G be a transitive abelian group of cyclic permutation matrices, referring to remark 7.6.1 it now follows that a cyclic permutation matrix $\dot{P}_k \varepsilon G$, $k \varepsilon Z_n$, has n distinct eigenvalues given by

$$\sigma^{j,k} = \gamma_n^{-jk} = \gamma_n^{n-jk} \quad ; \quad k, j \varepsilon Z_n , \qquad (7.6.8)$$

and that the eigenvector associated with the eigenvalue $\sigma^{j,k}$ is given by

$$\varphi^j = (1 \ \gamma_n^j \ \gamma_n^{2j} \dots \gamma_n^{\beta j} \dots \gamma_n^{(n-1)j})^T \quad ; \ \beta \varepsilon Z_n, \ j \varepsilon Z_n , \qquad (7.6.9)$$

where γ_n is a primitive n-th root of unity in Z_p and is given by equation (7.6.7).

Thus, the cyclic permutation matrices, P_k's, belonging to the transitive abelian group G of cyclic permutation matrices, have a common set of n eigenvectors given by equation (7.6.9).

We shall now show that these n eigenvectors provide a basis for the module M over Z_p. For this purpose, we first note that the set of elements $\{e_i\}$, $i \varepsilon Z_n$, where each e_i is an element of M with a 1 in the i-th position and zeros elsewhere, forms a basis for M, and that the eigenvectors of cyclic permutation matrices P_k's belonging to G given by equation (7.6.9) are written with respect to this basis. The n eigenvectors provide a basis for M if and only if the modal matrix formed by these eigenvectors is invertible [46 ,p.104]. The invertibility of the modal matrix has been shown in [47] in connection with the invertibility of NTT's. The eigenvectors (given by equation (7.6.9)) of the cyclic permutation matrices P_k's, belonging to G, therefore provide a basis for M. In other words, P_k's have a common set of linearly independent eigenvectors that generate M.

<u>Remark 7.6.4</u>: The invertibility of the modal matrix guarantees that its determinant has an inverse in the ring Z_p [46 ,p. 106].

Since any member of a class S of P-I systems is a linear combination of the P_k's [PR5 of A.6, Appendix A] it

follows that a class S of P-I systems has a common set of linearly independent eigenvectors that generate M. So, with these eigenvectors as a basis for M, the system matrix of every member of this class S takes a diagonal form.

We now give the following example to illustrate these ideas:

Example 7.6.3: Consider a cyclic P-I system with n = 2 over a module defined over the ring of residue class integers Z_{15}. The system matrix is $T = \begin{bmatrix} 8 & 5 \\ 5 & 8 \end{bmatrix}$, P = 15 = 3 x5. Therefore $p_0=3$, $p_1 = 5$; $Z_{15} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$. If (x,y) be the residue representation of any integer $w \varepsilon Z_{15}$, i.e., if $w \equiv x \bmod 3$ and $w \equiv y \bmod 5$, then by the CRT

$$w = |10.x + 6.y|_{15} .$$

Therefore, integers 0 to 14 belonging to Z_{15} have residue representations given in the following table:

Table 7.2: Residue Representation of ~~Numbers~~ Integers 0 to 14 in Example 7.6.3

w	(x,y)	w	(x,y)
0	(0,0)	9	(0,4)
1	(1,1)	10	(1,0)

Table 7.2: (continued)

w	(x,y)	w	(x,y)
2	(2,2)	11	(2,1)
3	(0,3)	12	(0,2)
4	(1,4)	13	(1,3)
5	(2,0)	14	(2,4)
6	(0,1)		
7	(1,2)		
8	(2,3)		

$$Z_3 = \{0,1,2\}, \text{ and } Z_5 = \{0,1,2,3,4\}.$$

The primitive 2nd root of unity in Z_3 is 2 and that is Z_5 is 4.

Hence, the primitive 2nd root of unity in Z_{15} is the one with (2,4) as its residue representation. Referring to Table 7.2, the primitive 2nd root of unity in Z_{15} is 14. i.e., $\gamma_2 = 14$.

Using equation(7.6.8), we may now write down the eigenvectors of the given class of cyclic P-I systems as

$$\varphi^0 = (1\ 1)^T,$$

and $\varphi^1 = (1\ 14)^T.$

The modal matrix is therefore

$$U = \begin{bmatrix} 1 & 1 \\ 1 & 14 \end{bmatrix} \quad \text{and} \quad U^{-1} = (13)^{-1} \begin{bmatrix} 14 & -1 \\ -1 & 1 \end{bmatrix} = 7 \begin{bmatrix} 14 & 14 \\ 14 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 8 \\ 8 & 7 \end{bmatrix}$$

$$U^{-1}TU = \begin{bmatrix} 8 & 8 \\ 8 & 7 \end{bmatrix} \begin{bmatrix} 8 & 5 \\ 5 & 8 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 14 \end{bmatrix} = \begin{bmatrix} 14 & 14 \\ 9 & 6 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 14 \end{bmatrix} = \begin{bmatrix} 13 & 0 \\ 0 & 3 \end{bmatrix}.$$

Thus, the modal matrix $\begin{bmatrix} 1 & 1 \\ 1 & 14 \end{bmatrix}$ diagonalizes the system matrix $\begin{bmatrix} 8 & 5 \\ 5 & 8 \end{bmatrix}$ yielding 13 and 3 as the eigenvalues of the system matrix.

7.6.3 Transform Pair Defined by Cyclic P-I Systems in Z_p

Recalling that the eigenvectors φ_n^j, $j\varepsilon Z_n$ span the n-dimensional module M defined over Z_p, an arbitrary signal $x = (x_0\ x_1\ \ldots.\ x_{n-1})^T \varepsilon M$ may be written as

$$x = X_0\ \varphi_n^0 + X_1\ \varphi_n^1 + \ldots. + X_{n-1}\ \varphi_n^{n-1} = \sum_{i=0}^{n-1} X_i\ \varphi_n^i ,$$

where X_i $i\varepsilon Z_n$ are scalars belonging to Z_p.

Therefore, the j-th component of x viz., x_j is given by

$$x_j = \sum_{i=0}^{n-1} X_i\ \varphi_n^{i,j} = \sum_{i=0}^{n-1} X_i\ \gamma_n^{ij} \quad ; \quad j\varepsilon Z_n , \tag{7.6.10}$$

where $\varphi_n^{i,j}$ is the j-th component of the i-th eigenvector φ_n^i and γ_n is a primitive n-th root of unity in Z_p.

Let the direct transform corresponding to 7.6.10 be of the form,

$$X_i = K \sum_{j=0}^{n-1} x_j \gamma_n^{-ij} \quad ; \quad i \varepsilon Z_n , \qquad (7.6.11)$$

where $K \varepsilon Z_p$ is a normalizing scalar the value of which is yet to be determined. Substituting (7.6.11) in (7.6.10) we get,

$$x_j = K \sum_{i=0}^{n-1} \gamma_n^{ij} \sum_{i=0}^{n-1} x_l \gamma_n^{-il}$$

$$= K \sum_{l=0}^{n-1} x_l \sum_{i=0}^{n-1} \gamma_n^{i(j-l)} .$$

Let $(j-l) = q$ then, we know that [47],

$$\sum_{i=0}^{n-1} \gamma_n^{iq} = \begin{cases} n & , \text{ if } q = 0 \bmod n \\ 0 & \text{otherwise} \end{cases} .$$

Therefore,

$$x_j = K \sum_{l=0}^{n-1} x_l \sum_{i=0}^{n-1} \gamma_n^{i(j-l)} = K x_j n .$$

This means that the normalizing constant K must be such that $Kn \equiv 1 \bmod P$, i.e., $K = \left| \frac{1}{n} \right|_P$

Thus, if n has a multiplicative inverse, say K, in Z_p, then

$$X_i \equiv (\sum_{j=0}^{n-1} x_j \gamma_n^{-ij}) \bmod P \quad ; \quad i \varepsilon Z_n , \tag{7.6.12}$$

and $$x_j \equiv (K \sum_{i=0}^{n-1} X_i \gamma_n^{ij}) \bmod P \quad ; \quad j \varepsilon Z_n . \tag{7.6.13}$$

Equations (7.6.12) and (7.6.13) give the finite discrete transform (FDT) pair defined by cyclic P-I systems on a ring Z_P.

7.6.4 Number-Theoretic Transforms

It may be observed that the FDT defined by cyclic P-I systems on Z_P has essentially the same structure as the familiar DFT pair. Further, just like the FDT defined by cyclic P-I systems on finite fields, and the DFT, the FDT pair of equations (7.6.12) and (7.6.13) also possesses cyclic convolutional property in that the pointwise product of the FDT of two finite sequences of equal length with entries from Z_P, is congruent to the FDT of the cyclic convolution of the two sequences. Thus, these transforms may be used for computing cyclic convolutions. When used for this purpose, they have an advantage over the DFT because in the computation of this transform, multiplication and addition of only integers is required and the arithmetic in the computation is carried out modulo P, where P is the modulus of the underlying ring Z_P.

If this modulus P of the ring Z_P is chosen to be a Mersenne number M_n given by

$$M_n = 2^n - 1,$$

where n is a prime, then 2 is the primitive n-th root of unity in Z_P. The FDT given by equations (7.6.12) and (7.6.13) and defined by cyclic P-I systems of dimension n on Z_P then gives the Mersenne number transform (MNT) proposed by Rader [16].

If, on the other hand, P, the modulus of the Z_P is a Fermat number F_t given by

$$F_t = 2^{2^t} + 1,$$

where t is any positive integer, then the FDT given by equations (7.6.12) and (7.6.13) and defined by cyclic P-I systems on Z_P, leads to the Fermat number transforms (FNT's) discussed in [19,20]. Thus,

Remark 7.6.5: For appropriate choice of P, the modulus of the ring of residue class integers Z_P, the FDT defined by cyclic class of P-I systems on Z_P gives rise to number theoretic transforms like the Mersenne number transforms and the Fermat number transforms.

7.6.5 General Classes of P-I Systems on Z_P

The study of P-I systems on rings has so far been concerned only with systems belonging to the cyclic class. The results obtained for this class may be extended to general classes of systems belonging to this category by following essentially the same arguments and procedures as were used in section 7.4. for obtaining the results pertaining to general classes of P-I systems on finite fields. The FDT pair defined by general classes of P-I systems on Z_P is then

$$X_k = \Big(\sum_{j=0}^{n-1} \bar{h}_n^{k,j}\, x_j\Big) \bmod P \quad ; \quad k\varepsilon Z_n\,, \qquad (7.6.14)$$

and
$$x_j = \Big(K \sum_{k=0}^{n-1} h_n^{k,j}\, X_k\Big) \bmod P \quad ; \quad j\varepsilon Z_n\,, \qquad (7.6.15)$$

where
$$h_n^{k,j} = \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{j_\alpha k_\alpha} \quad ; \quad j,\ k\varepsilon Z_n\,,$$

γ_{m_α} is the primitive m_α-th root of unity in Z_P,

m_α, $\alpha\varepsilon Z_r$ are the invariants of the group G relative to which the pertinent class of P-I systems is defined,

j_α and k_α are the mixed-radix digits in the expansion of j and k respectively with respect to the mixed-radices m_α, $\alpha\varepsilon Z_r$,

$\bar{h}_n^{k,j}$ is the multiplicative inverse in Z_P of $h_n^{k,j}$, and

K is the multiplicative inverse in Z_P of n.

Remark 7.6.6: The generalized FDT pair given by equations (7.6.14) and (7.6.15) and defined by general classes of P-I systems on Z_P are expected to be helpful in developing newer varities of NTT's which will have dyadic and such other non-cyclic convolutional properties.

CHAPTER 8

CONCLUSIONS

We have studied three new categories of permutation-invariant (P-I) systems as generalizations of the one-dimensional (1-D) P-I systems over real fields. These three new categories are

i. 2-D P-I systems whose input signals are 2-D arrays of reals of finite size,

ii. P-I systems on finite fields, whose input signals are finite-length sequences of elements drawn from finite fields, and

iii. P-I systems on rings, whose input signals are finite-length sequences of elements drawn from rings of residue class integers.

Systems belonging to the first category, i.e, 2-D P-I systems, have been studied in detail with regard to their sample domain as well as transform domain behaviour. In the

case of the next two categories, the main concern has been the transform domain behaviour, their sample domain behaviour being essentially the same as that of 1-D P-I systems with real-field inputs.

8.1 Summary of Results

Of the various results obtained in the study of these three new categories of systems, the main ones are the following:

i. 2-D P-I systems have been formally defined making use of two transitive abelian permutation groups, one for the rows and the other for the columns of the input signal array. Following the general practice in the study of systems, several characterizations of these 2-D P-I systems have been obtained. These include their characterizations in terms of the unit response matrices, generalized convolutional input-output relationships, eigen signals and generalized 2-D finite discrete transforms. The results on these characterizations depend centrally upon the fact that a class of 2-D P-I systems forms a vector space whose dimension is equal to that of the pertinent signal space on which that class operates.

ii. It is shown that just as the 1-D P-I systems are capable of spectrum shaping or filtering of 1-D finite discrete data, the 2-D P-I systems are likewise capable of filtering 2-D finite discrete data.

iii. A key result of the thesis is that for every class of 2-D P-I systems, there is a corresponding class of equivalent 1-D P-I systems. Hitherto, 1-D P-I systems belonging only to the cyclic and dyadic classes were known to have significant roles in the processing of finite discrete data. The result concerning the equivalence between 2-D and 1-D P-I systems brings out the fact that most of the other classes of 1-D P-I systems too have a significant role in the processing of finite discrete data since they are the 1-D equivalents of some two-dimensional or multidimensional P-I systems belonging either to the cyclic or dyadic classes. The usefulness of this equivalence between 2-D and 1-D P-I systems in the 1-D implementation of 2-D filters, has been demonstrated through several examples on 2-D Fourier domain and Walsh domain filtering. In establishing the equivalence between 2-D and 1-D P-I systems, use has been made of a generalized method of writing down the Kronecker product of matrices in order to obtain a unified treatment so that the results presented are equally valid irrespective of which particular linear transformation is used for obtaining the equivalent 1-D P-I system.

iv. Theories of P-I systems on finite fields and on rings, have been developed. In the process of evolving the theory of P-I systems on rings, a systematic procedure for determining the n-th roots of unity in rings of residue class integers, has been used.+ Characterizations of classes of these two new categories of

---

+ An application of the same procedure in proving the invertibility of NTT's has recently been reported by Vanwormhoudt [47].

systems in terms of the pertinent eigen signals and finite discrete transforms have been given. It has been shown that with an appropriate choice of the modulus of the ring of residue class integers, the transforms defined by the cyclic class of P-I systems on rings lead to the so-called number-theoretic transforms (NTT's) like the Mersenne number transform and the Fermat number transform, which have also been proposed during the last few years for efficient and error-free computation of convolutions. Transforms defined by other classes of P-I systems have been derived here and it is hoped that they would be helpful in evolving newer varieties of NTT's with dyadic and such other non-cyclic convolutional properties.

8.2 Scope for Further Research

Three distinct possibilities for further research are suggested by the results presented in this work.

i. Results on the equivalence between 2-D and 1-D P-I systems provide a new alternative to the problem of 2-D filtering using 1-D techniques. However, for a full and proper exploitation of these results, there is need for further investigation on two basic problems, namely, (a) the problem of approximation, particularly of the minimax kind, on discrete point sets, and (b) the problem of recursive realization of the 2-D transfer functions obtained by approximating the ideal.

ii. Linear sequential circuits (LSC's) are discrete-time LSI systems whose infinite length input and output sequences have their entries drawn from finite fields such as GF(2). For these LSC's a fault analysis procedure has in recent years been suggested [42] which is analogous to the well-known multifrequency techniques employed in the case of analogue circuits. It is based on a spectral-theoretic approach to the problem of fault analysis. Since P-I systems on finite fields are finite discrete counterparts of these LSC's, it is reasonable to expect that they will have analogous applications in the realization of digital systems. In that context, spectral-theoretic fault analysis techniques for P-I systems should be useful.

iii. Linear sequential circuits in the autonomous mode (ALSC's) generate output sequences that are inherently periodic; this periodic output for any given feedback structure of the ALSC, is dependent only on the initial conditions, or the initial state of the ALSC [48]. ALSC's are widely used for the generation of pseudo-random sequences. It appears that a P-I system formulation can be given to these ALSC's so that the same output sequence may be generated for the same initial conditions. If the usual concept of linear shift associated with the shift registers is replaced by permutations, then a generalized concept of LSC's based on the theory of P-I systems, is likely to emerge. Such a generalized concept may have useful applications in the generation of pseudo-random sequences. In this context, the results on the equivalence of 2-D and 1-D P-I systems, when extended to finite fields and rings, are likely to play an important role.

APPENDIX A

In this appendix, a summary of the theory of 1-D P-I systems with real field inputs [1] is given. It contains in some detail, all those results to which reference has been made in this thesis. Here, the mixed-radix number system is presented by the author of this thesis in the general setting of the theory of rings, in order to obtain in a more compact and well-knit manner several results derivable in terms of this number system.

A.1 Introduction to P-I Systems

The familiar cyclic and dyadic convolution systems, also called the cyclic and dyadic invariant systems, represent two very special cases of a more general family of classes of finite discrete linear systems in which members of each class of systems exhibit invariance in their input-output relationship to a particular chosen set of shifts or permutations of their input signals. When the pertinent input signals are of length n, these various sets of permutations are identified as transitive abelian groups of permutations of degree n, by imposing on them requirements similar to those possessed by the sets of time shifts in the case of LTI systems. Each transitive abelian permutation group of degree n is then used to define a class of permutation-invariant (P-I) systems of dimension n, where n denotes the length of the input signal.

Definition A.1: Let G be a transitive abelian permutation group of degree n and let p denote an element in G. Then a finite discrete linear system S is said to be permutation-invariant relative to G if for any signal $x \varepsilon R^n$,

$$p(Sx) = S(px). \tag{A.1}$$

Here, $p \varepsilon G$ is treated as an operator on R^n.

The set of all such systems relative to a given G is said to form a class of P-I systems of dimension n.

In the above definition, if G is a cyclic (dyadic) group, then the resulting class of P-I systems relative to G is known as the cyclic (dyadic) class of P-I systems. With classes of P-I systems defined as above, the number of classes of P-I systems of a given dimension n is simply equal to the number of distinct abstract abelian groups of order n, which may be enumerated using standard results in group theory.

In the study of P-I systems, cyclic groups have an important position. This is owing to the fact that any finite abelian group is the direct product of cyclic groups. We, therefore first consider some of the salient features of cyclic permutation groups in a brief manner.

A.2 Cyclic Permutation Groups

Let C be a cyclic group of permutation matrices of degree m. Then we order its elements in the following manner: that particular member of C, which by operating on an m-tuple shifts its zeroth element to the k-th position, is called P_k. Thus, the zeroth column of P_k has a 1 in its k-th position and zeros elsewhere, and all other columns of P_k are cyclic permutations of the zeroth column. It can then be seen that the (i,j)-th element $(P_k)_{i,j}$ of the cyclic permutation matrix $P_k \varepsilon G$ is given by:

$$(P_k)_{i,j} = \delta_{k,(i-j)_m} \qquad ; \qquad i,j,k \varepsilon Z_m \, , \tag{A.2}$$

where $(i-j)_m$ denotes modulo m subtraction of j from i. Equation (A.2) equivalently means that the i-th row of P_k has a 1 in the ℓ-th position where ℓ is given by

$$\ell = (i-k)_m \, . \tag{A.3}$$

Further,

$$P_k \cdot P_\ell = P_{(k+\ell)_m} \, . \tag{A.4}$$

We shall now use these properties of cyclic permutation groups in the indexing of finite abelian groups, with the help of what is called the mixed-radix number system.

A.3 Use of Mixed-Radix Number System in Indexing Finite Abelian Groups.

Let G be a finite abelian group of order n. Since any finite abelian group can be expressed as the direct product of its constituent primary cyclic components, let

$$G = C_{r-1} \overset{*}{X} C_{r-2} \overset{*}{X} - - X\, C_i \overset{*}{X} - - \overset{*}{X} C_0 \, , \tag{A.5}$$

where each C_i is a primary cyclic group of order m_i, $i\varepsilon Z_r$. The m_{r-1}, m_{r-2}, ---, m_0 are called the invariants of the finite abelian group G, and from (A.5) we have,

$$n = \prod_{i=0}^{r-1} m_i \, . \tag{A.6}$$

Now, consider the set of rings S_i, $i\varepsilon Z_r$, where each S_i is the ring of integers modulo m_i and in which addition and multiplication are defined to be with respect to modulo m_i. Thus, if $x, y\varepsilon S_i$,

$$x + y = (x + y)_{m_i} \, , \text{ and} \tag{A.7}$$

$$x . y \quad = (x \, . \, y)_{m_i} \, .$$

We may then construct a new ring S whose elements are the set of all ordered r-tuples:

$$a \overset{d}{=} \langle a_{r-1}, a_{r-2}, ---, a_0 \rangle \text{ with } a_i \varepsilon S_i, \; i\varepsilon Z_r . \tag{A.8}$$

If a , bεS, then, in the new ring S we define addition and multiplication as follows:

$$a + b = \langle a_{r-1}, a_{r-2}, ---, a_0\rangle + \langle b_{r-1}, b_{r-2}, ---, b_0\rangle$$
$$= \langle (a_{r-1} + b_{r-1})_{m_{r-1}}, (a_{r-2} + b_{r-2})_{m_{r-2}}, ---,$$
$$(a_0 + b_0)_{m_0}\rangle \qquad (A.9(a))$$

and,

$$a.b = \langle a_{r-1}, a_{r-2}, ---, a_0\rangle \cdot \langle b_{r-1}, b_{r-2}, ---, b_0\rangle$$
$$= \langle (a_{r-1}\cdot b_{r-1})_{m_{r-1}}, (a_{r-2}\cdot b_{r-2})_{m_{r-2}}, ---,$$
$$(a_0\cdot b_0)_{m_0}\rangle . \qquad (A.9(b))$$

The number of elements in S is equal to $\prod_{i=0}^{r-1} m_i = n$. Then, a possible one-to-one mapping between the set of integers 0,1, ---, (n-1) and the ring S is given by the rule

$$l = (m_{r-2}\cdot m_{r-3} --- m_0)a_{r-1} + (m_{r-3}\cdot m_{r-4} --- m_0)a_{r-2}$$
$$+ --- + (m_1\cdot m_0)\, a_2 + m_0\, a_1 + 1.a_0 , \qquad (A.10)$$

where $l\varepsilon Z_n$.

This rule or mapping permits us to represent uniquely any integer $l\varepsilon Z_n$ as an ordered r-tuple $\langle a_{r-1}, a_{r-2}, ---, a_1, a_0\rangle$ with $a_i \varepsilon S_i$, $i\varepsilon Z_r$, where each S_i is a ring of residue

class integers modulo m_i. The resulting representation is referred to as the mixed-radix representation of numbers with respect to the mixed radices m_i, $i \varepsilon Z_r$.

Now, let P_k^i be the k-th member of a cyclic group of permutation matrices of order m_i, this group being the regular representation of the cyclic group C_i in equation (A.5). Then, as explained below, a very convenient indexing scheme for the members of a finite abelian group G can be obtained using the mixed-radix number system.

With respect to the mixed radices $m_{r-1}, m_{r-2}, \cdots, m_0$ let $l \varepsilon Z_n$ have the representation

$$l = \langle l_{r-1}, l_{r-2}, \cdots, l_0 \rangle .$$

Using equation (A.5), a permutation matrix representation of G may be obtained in which the l-th member, denoted by P_l^G, is obtained as

$$P_l^G = P_{l_{r-1}}^{r-1} \otimes P_{l_{r-2}}^{r-2} \otimes \cdots \otimes P_{l_i}^{i} \otimes \cdots \otimes P_{l_0}^{0} , \tag{A.11}$$

where $P_{l_i}^i$ is a cyclic permutation matrix which is the l_i-th member of the cyclic group of permutation matrices of order m_i, and $\otimes$ denotes the ~~direct~~ product or Kronecker product of matrices. Now, in the group G, let

$$P_k^G \cdot P_l^G = P_p^G \qquad ; \qquad p,k,l \varepsilon Z_n . \tag{A.12}$$

Using equation (A.11), we may write

$$P_p^G = P_k^G \cdot P_l^G = (P_{k_{r-1}}^{r-1} \otimes \cdots \otimes P_{k_i}^i \otimes \cdots \otimes P_{k_0}^0)$$
$$\cdot (P_{l_{r-1}}^{r-1} \times \cdots \times P_{l_i}^i \times \cdots \times P_{l_0}^0) .$$

Using standard properties of Kronecker product, this may be written as

$$P_p^G = P_k^G \cdot P_l^G = (P_{k_{r-1}}^{r-1} \cdot P_{l_{r-1}}^{r-1}) \otimes \cdots \otimes (P_{k_i}^i \cdot P_{l_i}^i)$$
$$\otimes \cdots \otimes (P_{k_0}^0 \cdot P_{l_0}^0) .$$

Recalling that $P_{k_i}^i$, $k \varepsilon Z_n$, $i \varepsilon Z_r$ are all cyclic matrices and using equation (A.4)

$$P_p^G = P_k^G \cdot P_l^G = P^{r-1}_{(k_{r-1} + l_{r-1})_{m_{r-1}}} \otimes \cdots \otimes P^i_{(k_i + l_i)_{m_i}}$$
$$\otimes \cdots \otimes P^0_{(k_0 + l_0)_{m_0}} .$$

Then it follows from equation (A.11) that

$$p = \langle (k_{r-1} + l_{r-1})_{m_{r-1}}, (k_{r-2} + l_{r-2})_{m_{r-2}}, \cdots ,$$
$$(k_0 + l_0)_{m_0} \rangle \overset{d}{=} k \oplus l . \tag{A.13}$$

Thus, if a_i and a_j be any two elements of G, then

$$a_i \cdot a_j = a_{i \oplus j} \quad ; \qquad i, j \varepsilon Z_n , \tag{A.14}$$

where $i \oplus j$ denotes point-wise addition of the integers i and j belonging to Z_n in the mixed-radix number system with

radices $m_{r-1}, m_{r-2}, \cdots, m_0$. In other words, the abstract abelian group G of order n with invariants $m_{r-1}, m_{r-2}, \cdots, m_0$ is completely specified by the rule of composition for the group elements as stated by equation (A.14).

Further, using this indexing scheme for members of G, the effect of permuting a given n-tuple $x = (x_0\ x_1 \cdots x_{n-1})^T$ by any member $P_k^G \in G$ may be stated in a compact way as we shall presently see. From equation (A.11) it follows that the j-th row of P_k^G is the direct product of the j_{r-1}-th row of $P_{k_{r-1}}^{r-1}$, j_{r-2}-th row of $P_{k_{r-2}}^{r-2}$, $\cdots$ and the j_0-th row of $P_{k_0}^0$. As seen from equation (A.4), the j_α-th row of $P_{k_\alpha}^\alpha$ has a 1 in the $(j_\alpha - k_\alpha)_{m_\alpha}$-th position and has zeros every where else. Therefore, the j-th row of P_k^G has a 1 in the $(j_{r-1} - k_{r-1})_{m_{r-1}}$ $(j_{r-2} - k_{r-2})_{m_{r-2}} \cdots, (j_\alpha - k_\alpha)_{m_\alpha}, \cdots, (j_0 - k_0)_{m_0}$ -th ? i.e., (j - k)-th position and zeros every where else.

Then it immediately follows that if

$$y = P_k^G\, x \text{ where } x = (x_0\ x_1 \cdots x_{n-1})^T,$$

then,

$$(y)_j = x_{j \ominus k} \tag{A.15}$$

i.e., the j-th element of y is given by $x_{j \ominus k}$ where $\ominus$ denotes subtraction in the mixed-radix system of numbers, with the invariants of G viz., $m_{r-1}, m_{r-2}, \cdots, m_0$ as the mixed radices.

Next in importance to the method of ordering members of G using the mixed-radix system, is the set of basic properties of these members of G.

A.4 Properties of Permutation Matrices

Let G be a transitive abelian group of permutation matrices P_k, $k\epsilon Z_n$. Then

PR1 : $P_j \; P_k = P_k \; P_j = P_{j \oplus k}$; $j, k\epsilon Z_n$.

PR2 : The set M of matrices P_k, $k\epsilon Z_n$, is linearly independent.

PR3 : The matrices P_k, $k\epsilon Z_n$, are orthogonal and hence normal.

PR4 : The matrices P_k, $k\epsilon Z_n$, are periodic matrices, that is $P_k^s = I$ for some integer s; the superscript s denotes the s-th power of the matrix P_k.

PR5 : The n x n matrix P_k, $k\epsilon Z_n$ is equal to the direct product of cyclic permutation matrices Q_{k_α} of orders m_α, $\alpha\epsilon Z_r$, and $\prod_{\alpha=0}^{r-1} m_\alpha = n$. That is

$$P_k = Q_{k_{r-1}} \otimes \cdots \otimes Q_{k_\alpha} \otimes \cdots \; Q_{k_0} \; ; \qquad 0 \leq k_\alpha < m_\alpha \; ; \; \alpha\epsilon Z_r \; , \tag{A.16}$$

where k_α, $\alpha\epsilon Z_r$ are the mixed-radix digits in the mixed-radix representation of $k\epsilon Z_n$ with respect to mixed-radices m_α, $\alpha\epsilon Z_r$.

A.5 Sample Domain Characterization of P-I Systems

Let S be a P-I system defined relative to a transitive abelian group G of permutation matrices, the order of the group being n. Therefore, the input signals of S are members of R^n. Let the set e_j, $j \varepsilon Z_n$ be the standard basis of R^n. Then an arbitrary input signal $x \varepsilon R^n$ may be written as

$$x = \sum_{j=0}^{n-1} x_j \, e_j \, .$$

Therefore,

$$y = S\left(\sum_{j=0}^{n-1} x_j \, e_j\right) = \sum_{j=0}^{n-1} x_j \, S \, e_j \, .$$

But since $e_j = P_j \, e_0$; $P_j \varepsilon G$, and $S \, P_j = P_j S$ from equation (A.1)

$$y = \sum_{j=0}^{n-1} x_j \, S \, P_j \, e_0 = \sum_{j=0}^{n-1} x_j \, P_j \, S \, e_0 \, .$$

If we call $e_0 = (1,0, \cdots, 0)^T$ as the unit sample signal then $S \, e_0$ represents the system's unit sample response. Let

$$s^{(0)} \stackrel{d}{=} S \, e_0 \, .$$

Then,

$$y = \sum_{j=0}^{n-1} x_j \, P_j \, s^{(0)} .$$

Using equation (A.15), this may now be written: as

$$y_i = \sum_{j=0}^{n-1} x_j \, s_{i \ominus j} \qquad ; \quad i \varepsilon Z_n ; \; s_k \varepsilon s^{(0)}, k \varepsilon Z_n \, . \qquad (A.17)$$

The formula given by equation (A.17), called the generalized convolutional relationship, is comparable to the ordinary discrete convolutional relationship characterizing discrete LTI systems. In this equation, $i \ominus j$ denotes point-wise subtraction of j from i in the mixed-radix system of representation of i and j with respect to the mixed radices $m_{r-1}, m_{r-2}, \ldots, m_0$ that are the invariants of group G relative to which the P-I system has been defined. It can easily be verified that for the special case of G being a cyclic (dyadic) group, equation (A.17) takes the form of a cyclic (dyadic) convolutional relationship.

With respect to the standard basis for R^n, equation (A.17) takes the matrix form

$$y = Sx,$$

where S, called the system matrix or P-I matrix, is defined as

$$S = (s_{i \ominus j}) \quad ; \quad i,j \varepsilon Z_n; \; s_k \varepsilon S^{(0)}; \; k \varepsilon Z_n . \tag{A.18}$$

A.6 Properties of P-I Matrices

The P-I matrix defined as in (A.18) has the following properties:

PR1 : The zeroth column of any P-I matrix represents the unit sample response $S^{(0)}$ of the P-I system represented by it.

PR2 : The k-th column $S^{(k)}$ of any P-I matrix S is given by $S^{(k)} = P_k S^{(0)}$, where $P_k \varepsilon G$, $k \varepsilon Z_n$, G being the transitive abelian permutation group relative to which the P-I system S is defined.

PR3 : The principal diagonal elements of any P-I matrix are all equal to its (0,0)-th element.

PR4 : P-I matrices are symmetrical about their secondary diagonal.

PR5 : Any n x n matrix S is a P-I matrix iff it is a a linear combination of the permutation matrices $P_k \varepsilon G$, $k \varepsilon Z_n$, where G is a transitive abelian permutation group.

PR6 : P-I matrices of order n representing a class of P-I systems of dimension n, defined with respect to a transitive abelian permutation group G, constitute a vector space of dimension n; the set M of matrices P_k, $k \varepsilon Z_n$, representing elements of the group G, is a basis of this vector space.

It was mentioned earlier (PR3 of permutation matrices) that the permutation matrices $P_k \varepsilon G$ are normal and we know they commute pairwise being members of an abelian group. They are therefore unitarily similar to diagonal matrices. In other words, P_k's have a common set of n linearly independent eigen vectors that are pairwise orthogonal. Then from property PR6 of P-I matrices, it follows that

PR7 : The n x n P-I matrices representing a class of P-I systems, have a common set of n linearly independent pairwise orthogonal eigenvectors.

PR8 : The eigenvalues of P-I matrices are linear combinations of roots of unity.

A.7 Eigenvalues and Eigenvectors of P-I Matrices

It is known that a cyclic permutation matrix such as $Q_{k\alpha}$ of order m_α (refer to equation A.16) has the following set of m_α eigenvectors $\varphi^{\beta}_{m_\alpha}$, $\beta \varepsilon Z_{m_\alpha}$ and eigenvalues $\sigma^{P,k_\alpha}_{m_\alpha}$, $\beta,\ k_\alpha \varepsilon Z_{m_\alpha}$:

$$\varphi^{\beta}_{m_\alpha} = (1\ \gamma^{\beta}_{m_\alpha}\ \gamma^{2\beta}_{m_\alpha} --- \gamma^{k_\alpha\beta}_{m_\alpha} --- \gamma^{(m_\alpha-1)\beta}_{m_\alpha})^T ;$$

$$k_\alpha,\ \beta\varepsilon Z_{m_\alpha},\ \alpha\varepsilon Z_r , \tag{A.19}$$

and

$$\sigma^{\beta,k_\alpha}_{m_\alpha} = \gamma^{-\beta k_\alpha}_{m_\alpha} \quad ; \quad \beta,\ k_\alpha\varepsilon Z_{m_\alpha},\ \alpha\varepsilon Z_r , \tag{A.20}$$

where,

$$\gamma_{m_\alpha} = \exp(\sqrt{-1}\ \frac{2\pi}{m_\alpha}) . \tag{A.21}$$

Thus, the modal matrix of Q_{k_α} is given by

$$u_{m_\alpha} = [\ \varphi^{0}_{m_\alpha} \mid \varphi^{1}_{m_\alpha} \mid --- \mid \varphi^{\beta}_{m_\alpha} \mid --- \mid \varphi^{m_\alpha-1}_{m_\alpha}] . \tag{A.22}$$

Since P_k equals the direct product of the cyclic permutation matrices Q_{k_α}, $k_\alpha\varepsilon Z_{m_\alpha}$, $\alpha\varepsilon Z_r$, it follows that each P_k, $k\varepsilon Z_n$

belonging to G has a modal matrix H_n which is the direct product of the modal matrices of its constituent cyclic per- mutation matrices Q_{k_α} ; $k_\alpha \varepsilon Z_{m_\alpha}$, $\alpha \varepsilon Z_r$. Therefore, the j-th eigenvector h_n^j of any P_k is equal to the direct product of j_{r-1}-th, j_{r-2}-th, - - - , j_α-th - - - and j_0-th (where j_α, $\alpha \varepsilon Z_r$ are the mixed-radix digits in the expansion of $j \varepsilon Z_n$ with respect to the mixed radices m_α, $\alpha \varepsilon Z_r$) eigenvectors of $Q_{k_{r-1}}$, - - - , Q_{k_α}, - - - and Q_{k_0} respectively. Therefore,

$$h_n^j = \varphi_{m_{r-1}}^{j_{r-1}} \times --- \times \varphi_{m_\alpha}^{j_\alpha} \times --- \times \varphi_{m_0}^{j_0} \; ; \; j \varepsilon Z_n \, , \tag{A.23}$$

where,

$$\varphi_{m_\alpha}^{j_\alpha} = (1 \;\; \gamma_{m_\alpha}^{j_\alpha} \;\; \gamma_{m_\alpha}^{2j_\alpha} \; - - - \; \gamma_{m_\alpha}^{\beta j_\alpha} - - - \gamma_{m_\alpha}^{(m_\alpha-1) j_\alpha})^T \; ;$$

$$j_\alpha \, , \; \beta \varepsilon Z_{m_\alpha} \; ,$$

and,

$$\gamma_{m_\alpha} = \exp(\sqrt{-1}\, \frac{2\pi}{m_\alpha}) \; , \; \alpha \varepsilon Z_r .$$

Therefore, the i-th component of h_n^j, viz., $h_n^{i,j}$ is given by

$$\begin{aligned} h_n^{i,j} &= \gamma_{m_{r-1}}^{i_{r-1} j_{r-1}} - - \gamma_{m_\alpha}^{i_\alpha j_\alpha} - - \gamma_{m_0}^{i_0 j_0} \\ &= \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{i_\alpha j_\alpha} \, , \end{aligned} \tag{A.24}$$

where, i_α, $\alpha \varepsilon Z_r$ are the mixed-radix digits in the expansion of $i \varepsilon Z_n$ with respect to the mixed radices m_α, $\alpha \varepsilon Z_r$.

Likewise, the j-th eigenvalue $\sigma_n^{j,k}$ of P_k is equal to the product of j_{r-1}-th, - --, j_α-th, --- and j_0-th eigenvalues of its constituent cyclic permutation matrices $Q_{k_{r-1}}$, $Q_{k_{r-2}}$, - --, Q_{k_α}, - -- and Q_{k_0} respectively. Therefore,

$$\sigma_n^{j,k} = \sigma_{m_{r-1}}^{j_{r-1},k_{r-1}} - - \sigma_{m_\alpha}^{j_\alpha,k_\alpha} - - \sigma_{m_0}^{j_0,k_0}.$$

But since $\sigma_{m_\alpha}^{j_\alpha,k_\alpha} = \gamma_{m_\alpha}^{-j_\alpha k_\alpha}$, $\alpha \varepsilon Z_r$ (refer to equation A.20), we have,

$$\sigma_n^{j,k} = \gamma_{m_{r-1}}^{-j_{r-1}k_{r-1}} - - \gamma_{m_\alpha}^{-j_\alpha k_\alpha} - - \gamma_{m_0}^{-j_0 k_0}$$

$$= \prod_{\alpha=0}^{r-1} \gamma_{m_\alpha}^{-j_\alpha k_\alpha} = \bar{h}_n^{j,k}, \tag{A.25}$$

where, $\bar{h}_n^{j,k}$ is the complex conjugate of $h_n^{j,k}$.

As mentioned earlier, P_k's are simultaneously diagonalizable, and the pertinent modal matrix H_n is then given by

$$H_n = [h_n^0 \mid h_n^1 \mid - - \mid h_n^j \mid - - \mid h_n^{n-1}], \tag{A.26}$$

where h_n^j, the j-th eigenvector is given by equation (A.23).

Remark 1: The eigenvectors h_n^j, $j\varepsilon Z_n$, constituting the columns of the modal matrix H_n are Levy's discrete generalized Walsh functions.

Remark 2: The modal matrices H_n belong to the family of generalized Hadamard matrices introduced by Butson, and are symmetric and in the standard form.

Remark 3: The modal matrix H_n satisfies the relationship $H_n H_n^* = nI_n$ where H_n^* denotes the complex conjugate transpose of H_n and I_n is the n x n identity matrix. Thus $H_n^{-1} = \frac{1}{n} H_n^*$.

Remark 4: From properties PR6 and PR7 of the P-I matrices, it follows that h_n^j, $j \varepsilon Z_n$ constitute a set of n pairwise orthogonal linearly independent eigenvectors common to the entire class of P-I systems defined with respect to the transitive abelian group of permutations, G.

A.8 Generalized Walsh-Hadamard Transforms

The eigenvectors h_n^j, $j \varepsilon Z_n$ being linearly independent, constitute a basis for the n-tuples $x = (x_0, x_1, ---, x_{n-1})$ in C^n. That is, we have

$$x = \frac{1}{n} \sum_{j=0}^{n-1} X_j \, h_n^j .$$

This may equivalently be written as

$$x = \frac{1}{n} H_n X , \tag{A.27}$$

where,

$$H_n = [h_n^0 \mid h_n^1 \mid \cdot \cdot \cdot \mid h_n^{n-1}] ,$$

and,

$$X = (X_0\ X_1\ -\ -\ X_{n-1})^T.$$

By referring to Remark 3, we may now write

$$X = H_n^* x . \tag{A.28}$$

Equations (A.27) and (A.28) can alternatively be expressed in the form

$$x_j = \frac{1}{n} \sum_{k=0}^{n-1} h_n^{j,k} X_k \ ; \qquad j \varepsilon Z_n \ , \tag{A.29}$$

and

$$X_k = \sum_{j=0}^{n-1} \bar{h}_n^{k,j} x_j \qquad ; \qquad k \varepsilon Z_n \ . \tag{A.30}$$

Definition A.2: The pair of equations (A.27) and (A.28), or alternatively (A.29) and (A.30) will be called the generalized Walsh-Hadamard transform (GWHT) pair. X will be said to be the GWHT of x, and x the inverse GWHT of X.

Remark 5: The matrices associated with the DFT and DWT are special cases of the generalized Hadamard matrix H_n. Consequently, the DFT and DWT are themselves special cases of the GWHT.

Remark 6: A generalization of the DFT and DWT, the GWHT satisfies a generalized convolution theorem which states that the GWHT of the generalized convolution of two signals

(n-tuples) is equal to the pointwise product of the generalized Walsh Hadamard transform of the individual signals. Thus, if the generalized convolution of two signals s and x is given by

$$y_i = \sum_{j=o}^{n-1} s_{i \ominus j}\, x_j \qquad ; \quad i \varepsilon Z_n , \qquad (A.31)$$

then,

$$Y_k = S_k . X_k \qquad ; \quad k \varepsilon Z_n , \qquad (A.32)$$

where, Y_k, S_k, and X_k are the k-th components of the GWHT's of respectively y, s, and x.

From equation (A.32) of remark 6 it follows that the transfer function of a P-I system may simply be taken as the generalized Walsh Hadamard transform of its unit sample response.

APPENDIX B

KRONECKER PRODUCT OF MATRICES

This appendix gives some useful results pertaining to the Kronecker product of matrices [31,41,49]. A generalized method of writing down the product matrix is discussed and some of the important properties of the Kronecker products are given.

B.1 Kronecker Product Matrix

If A is an m x n matrix and B is a p x q matrix, the Kronecker product of A and B (in that order), denoted by $A \otimes B$, is generally defined to be the mp x nq matrix given by

$$A \otimes B = \begin{bmatrix} a_{0,0}B & a_{0,1}B \cdots\cdots a_{0,n-1}B \\ a_{1,0}B & a_{1,1}B \cdots\cdots a_{1,n-1}B \\ \vdots & \vdots \qquad\qquad \vdots \\ a_{m-1,0}B & a_{m-1,1}B \cdots a_{m-1,n-1}B \end{bmatrix}.$$

This method of writing down the product matrix makes use of the lexicographic way of ordering of pairs of indices [41]. In this thesis, a more general way of writing down the Kronecker product of matrices is made use of. In this method, the product matrix of two permutation matrices p_r of size m x m and q_s of size n x n is written down making

use of a one-to-one index mapping f

$$f : Z_m \times Z_n \rightarrow Z_N \quad ; \quad N = m.n$$

This product is denoted here by the symbol $\otimes_Q$.

In writing down this Kronecker product matrix, we note that the k-th column of the product matrix is obtained by taking the Kronecker product $p_r^i \otimes_Q q_s^j$ where p_r^i is the i-th column of the matrix p_r and q_s^j is the j-th column of the matrix q_s. Values of k corresponding to particular values of i and j, $i \epsilon Z_m$, $j \epsilon Z_n$, are obtained by using the index mapping f. The l-th element of this k-th column of the product matrix is obtained by taking the product of the t-th element of p_r^i and the u-th element of q_s^j where $(t,u) = f^{-1}(l)$.

B.2 Properties of Kronecker Products

PR1. $(A_1 + A_2) \otimes B = (A_1 \otimes B) + (A_2 \otimes B)$

PR2. $A \otimes (B_1 + B_2) = (A \otimes B_1) + (A \otimes B_2)$

PR3. $\alpha A \otimes \beta B = \alpha\beta \; (A \otimes B)$

PR4. $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$

PR5. $(A_1 \; A_2) \otimes (B_1 \; B_2) = (A_1 \otimes B_1) \; (A_2 \otimes B_2)$

REFERENCES

1. Siddiqi, M.U., 'A Study of Permutation-invariant Linear Systems', Ph.D. thesis, Department of Electrical Engineering, June, 1976, Indian Institute of Technology, Kanpur.

2. Gethöffer, H., 'Mutual Mappings of Generalized Convolution Systems', Proc. 1972 Symp. Appl. Walsh Functions, Washington, pp. 310-317.

3. Rasenbloom, J.H., 'Physical Interpretation of Dyadic Groups', Proc. 1971 Symp. Appl. Walsh Functions, Washington, pp. 158-165.

4. Cheng, D.K., and Liu, J.J., 'Time-domain Analysis of Discrete Dyadic-invariant Systems', Proc. IEEE, Vol. 62, pp. 1038-1040, July, 1974.

5. Cheng, D.K., and Liu, J.J., 'Walsh Transform Analysis of Discrete Dyadic-invariant Systems', IEEE Trans. Vol. EMC-16, pp. 136-140, May, 1974.

6. McClellan, J.H., 'The Design of Two-dimensional Digital Filters by Transformations', Proc. 7th Annu. Princeton Conf. on Inform. Sci. and Syst., March, 1973, pp. 247-251.

7. Treitel, S., and Shanks, J.L., 'The Design of Multistage Separable Planar Filters', IEEE Trans. Geosci. Electron., Vol. GE-9, pp. 10-27, Jan. 1971.

8. Mersereau, R.M., and Dudgeon, D.E., 'Two Dimensional Digital Filtering', Proc. IEEE, Vol. 63, No. 4, pp. 610-623, April, 1975.

9. Shanks, J.L., Treitel, S., and Justice, J.H., 'Stability and Synthesis of Two-dimensional Recursive Filters', IEEE Trans. on Audio and Electroacoustics, AU-20, No. 2, pp. 115-128, June, 1972.

10. Huang, T.S., 'Stability of Two-dimensional Recursive Filters', IEEE Trans. on Audio and Electroacoustics, AU-20, No. 2, pp. 158-163, June, 1972.

11. Anderson, B.D., and Jury, E.I., 'Stability Test for Two-dimensional Recursive Filters', IEEE Trans. on Audio and Electroacoustics, AU-21, No. 4, pp. 366-372, Aug., 1973.

12. Ekstrom, M.P., and Woods, J.W., 'Two-dimensional Spectral Factorization with Applications in Recursive Digital Filtering', IEEE Trans. Vol. ASSP-24, No. 2, April, 1976.

13. Manry, M.T., and Agarwal, J.K., 'Picture Processing using One-dimensional Implementations of Discrete Planar Filters', IEEE Trans. Acoust. Speech, Sig. Proc. Vol. ASSP-22, pp. 164-173, June, 1974.

14. Cooley, J.W., and Tukey, J.W., 'An Algorithm for the Machine Calculation of Complex Fourier Series,' Math. Comp., Vol. 19, No. 90, pp. 297-301, 1965.

15. Pollard, J.M., 'The Fast Fourier Transform in a Finite Field', Math. Comput. Vol. 25, pp. 365-374, April, 1971.

16. Rader, C.M., 'Discrete Convolutions via Mersenne Transforms', IEEE Trans. Comput., Vol. C-21, pp. 1269-1273, Dec. 1972.

17. Agarwal, R.C., and Burrus, C.S., 'Fast Digital Convolutions using Fermat Transforms', Southwest IEEE Conf. Rec. pp. 538-543, April, 1973.

18. Nussbaumer, H., 'Digital Filtering using Pseudo Fermat Number Transforms', IEEE Trans. Acoustics, Speech, and Signal Processing, Vol. ASSP-25, No. 1, pp. 79-83, Feb., 1977.

19. Agarwal, R.C., and Burrus, C.S., 'Fast Convolution using Fermat Number Transforms with Applications to Digital Filtering', IEEE Trans. Acoust. Speech, Signal Processing, Vol. ASSP-22, pp. 87-97, April, 1974.

20. Agarwal, R.C., and Burrus, C.S., 'Number Theoretic Transforms to Implement Fast Digital Convolutions', Proc. IEEE, Vol. 63, pp. 550-560, April, 1975.

21. Nussbaumer, H.J., 'Complex Convolutions via Fermat Number Transforms', IBM J. Res. Develop., Vol. 20, pp. 282-284, May, 1976.

22. Burnside, W., Theory of Groups of Finite Order, Dover Publications, New York, 1955.

23. Carmichael, R.D., Introduction to the Theory of Groups of Finite Order, Dover Publications, New York, 1956.

24. Schmidt, O.U., Abstract Theory of Groups (English Translation), W.H. Freeman Company, San Francisco,

25. Kochendörffer, R., Group Theory (English Translation), McGraw-Hill, London, 1970.

26. Ledermann, W., Introduction to Group Theory, Oliver and Boyd, Edinburgh, 1973.

27. Zassenhaus, H., The Theory of Groups, Chelsea, 1958.

28. Hall, M., The Theory of Groups, Macmillan, New York, 1959.

29. Curtis, C.W., Reiner, I., 'Representation Theory of Finite Groups and Associative Algebras', Interscience Publishers, 1962.

30. Kenneth Hoffman, and Ray Kunze, 'Linear Algebra', (Second Edition), Prentice-Hall of India, New Delhi, 1975.

31. Bellman, R., 'Introduction to Matrix Analysis', McGraw Hill Book Company, Inc., 1960.

32. Burrus, C.S., 'Index Mappings for Multidimensional Formulation of the DFT and Convolution', IEEE Trans. Acoust. Speech, Signal Processing, Vol. ASSP-25, No. 3, pp. 239-242, June, 1977.

33. Cooley, J.W., Lewis, P.A.W., and Peter D. Welch., 'Historical Notes on the Fast Fourier Transform', IEEE Trans. Audio Electroacoust, Vol. AU-15, pp. 76-79, June, 1967.

34. Gullick, and Davidson, 'Abstract Algebra', Haughton and Mifflin Company, 1976.

35. Butson, A.T., 'Generalized Hadamard Matrices', Proc. Amer. Math. Soc., Vol. 13, No. 6, pp. 894-898, Dec. 1962.

36. Ahmed, N., Schreiber, H.H., and Lopresti, P.V., 'On Notation and Definition of Terms Related to a Class of Complete Orthogonal Functions', IEEE Trans., Vol. EMC-15, No. 2, pp. 75-80, May 1973.

37. Pratt, W.K., Kane, J., and Andrews, H., 'Hadamard Transform Image Coding', IEEE Proc. Vol. 57, No. 1, Jan. 1969.

38. Cochran, W.T., et.al., 'What is Fast Fourier Transform', IEEE Trans. Vol. AU-15, No. 2, pp. 45-55, June 1967.

39. Beauchamp, K.G., 'Walsh Functions and their Applications', Academic Press, 1975.

40. Rabiner. L.R., and Gold, B., 'Theory and Applications of Digital Signal Processing', Prentice-Hall, New Jersey, 1975.

41. Halmos, P.R., 'Finite Dimensional Vector Spaces' (East-West Edition), Affiliated East-West Press, New Delhi, 1974.

42. Sangani, S.H., Saeks, R., and Liberty, S.R., 'A Spectral Theoretic Approach to Fault Analysis in Linear Sequential Circuits', Journal of the Franklin Institute, Vol. 302, No. 3, pp. 239-258, September, 1976.

43. Key, E.L., 'An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators', IEEE Trans. Inf. Theory, Vol. IT-22, No. 6, pp. 732-736, November, 1976.

44. Szabo', N.S., and Tanaka, R.I., 'Residue Arithmetic and its Applications to Computer Technology', McGraw-Hill Book Company, 1967.

45. Ribenboin, P., 'Rings and Modules', Interscience Publishers, 1969.

46. Hartley, B., and Hawkes, T.O., 'Rings, Modules and Linear Algebra', Chapman and Hall, 1970.

47. Vanwormhoudt, M.C., 'On Number Theoretic Fourier Transforms in Residue Class Rings', IEEE Trans. Acoust, Speech, Signal Processing, Vol. ASSP-25, No. 6, pp. 585-586, Dec., 1977.

48. Gill, A., 'Linear Sequential Circuits -- Analysis, Synthesis and Applications', McGraw-Hill Book Company, 1967.

49. Lancaster, P., 'Theory of Matrices', Academic Press, New York, 1969.